Dossier Pédagogique

BTS SIO SISR

Maho Guezenec
Candidat: 02541481976

La Région Bretagne - DNSI SINFRA

Table des matières

Tableau des compétences

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS		SESSION 2026
Tableau de synthèse des réalisations professionnelles		
NOM et prénom : GUEZENEC MAHO		N° candidat : 02541481976
Centre de formation : CMA FORMATION BRETAGNE		Option : ☑ SISR ☐ SLAM
Lien Portefeuille de compétences : https://maho-guezenec.com		

Compétences mises en œuvre / *Réalisations professionnelles (intitulé et liste des documents et productions associés)*	Période (sous la forme du JJ/MM/AA au JJ/MM/AA)	Gérer le patrimoine informatique	Répondre aux incidents et aux demandes d'assistance et d'évolution	Développer la présence en ligne de l'organisation	Travailler en mode projet	Mettre à disposition des utilisateurs un service informatique	Organiser son développement professionnel
		• Recenser et identifier les ressources numériques • Exploiter des référentiels, normes et standards adoptés par la prestataire informatique • Mettre en place et vérifier les niveaux d'habilitation associés à un service • Vérifier les conditions de la continuité d'un service informatique • Gérer des sauvegardes • Vérifier le respect des règles d'utilisation des ressources numériques	• Collecter, suivre et orienter des demandes • Traiter des demandes concernant les services réseau et système, applicatifs • Traiter des demandes concernant les applications	• Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques • Référencer les services en ligne de l'organisation et mesurer leur visibilité. • Participer à l'évolution d'un site Web exploitant les données de l'organisation.	• Analyser les objectifs et les modalités d'organisation d'un projet • Planifier les activités • Évaluer les indicateurs de suivi d'un projet et analyser les écarts	• Réaliser les tests d'intégration et d'acceptation d'un service • Déployer un service • Accompagner les utilisateurs dans la mise en place d'un service	• Maîtriser son environnement d'apprentissage personnel • Mettre en œuvre des outils et stratégies de veille informationnelle • Gérer son identité professionnelle • Développer son projet professionnel
Réalisation en cours de formation							
Réalisation du port-folio							X
Réalisations en milieu professionnel en cours de première année							
Intervention au data center de TDF à Cesson-Sévigné	15/10/2024 au 18/10/2024	X				X	
Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy	04/11/2024 au 29/11/2024		X	X	X	X	
Déploiement de LibreNMS (outil de supervision)	13/01/2025 au 23/02/2025	X			X		
Réalisations en milieu professionnel en cours de seconde année							
Déploiement de HPE IMC sur le parc institutionnel	06/09/2025 au 31/08/2026	X			X		X
Projet MAN et segmentation de l'infrastructure	2024 - 2026	X	X		X		X
Installation d'une salle de visioconférence avec Vidélio	02/08/2025 au 06/08/2025		X		X	X	
Veille technologique sur le FortiAI	2024 - 2026						X

Introduction

Ce dossier présente un aperçu des activités que j'ai réalisées au sein de la région Bretagne durant mes deux dernières années, en poste d'apprenti SIO au sein de la DNSI, dans le service SINFRA, et plus particulièrement au sein de l'équipe Réseau.

Au cours de cette période, j'ai eu l'occasion de participer à de nombreuses missions variées, touchant à la fois à la gestion des infrastructures réseau, à la maintenance des équipements, à l'optimisation des services et au suivi des projets techniques.

Pour rendre ce dossier plus clair et synthétique, j'ai choisi de condenser mon expérience en six activités principales, chacune illustrant des compétences techniques et professionnelles que j'ai pu développer. Ces missions m'ont permis d'acquérir de solides connaissances, de renforcer mes capacités d'analyse et de résolution de problèmes, et de mieux comprendre le fonctionnement d'une grande organisation numérique telle que celle de la région Bretagne.

Elles témoignent également de mon évolution personnelle et de mon engagement dans l'équipe Réseau, où j'ai appris à travailler en collaboration, à gérer des priorités et à m'adapter à des situations variées. Ce document a donc pour objectif de présenter ces expériences marquantes et de montrer comment elles ont contribué à mon apprentissage et à ma progression professionnelle au cours de ces deux années.

Région BRETAGNE DNSI

Pour des raisons de confidentialité, toutes les adresses IP, VLAN et autres informations sensibles présentes dans ce dossier ont été modifiées.

Ces changements n'affectent en rien le travail réalisé ni les résultats présentés.

Curriculum Vitae

La Région Bretagne

Région Bretagne, 283 Avenue du Général Patton, 35000

J'ai effectué mon alternance au sein de la Région Bretagne, une collectivité territoriale majeure qui intervient dans de nombreux domaines publics tels que la gestion des lycées, les transports régionaux, le développement économique, l'aménagement du territoire et la transition numérique. Pour assurer le bon fonctionnement de l'ensemble de ses services, la Région s'appuie sur une infrastructure informatique centralisée et sécurisée, pilotée par la DNSI (Direction du Numérique et des Systèmes d'Information).

Au sein de la DNSI, j'ai intégré le service Réseau, une équipe composée de plusieurs ingénieurs et techniciens réseaux spécialisés dans la gestion des infrastructures, la sécurité périmétrique, la connectivité des sites distants et la supervision des équipements. L'équipe est responsable du maintien en condition opérationnelle des équipements réseau (switchs, routeurs, firewalls), de la gestion des interconnexions entre les différents sites régionaux ainsi que de la sécurisation des flux de données. Elle intervient également sur les data centers hébergeant les services critiques.

Mon intégration dans cette équipe m'a permis de découvrir un environnement professionnel structuré, avec des procédures précises, des contraintes fortes en matière de sécurité et une exigence élevée en termes de disponibilité des services. Travailler aux côtés d'ingénieurs réseaux m'a offert l'opportunité d'approfondir mes compétences techniques, de mieux comprendre les enjeux liés à la continuité de service et de participer à des projets concrets ayant un impact direct sur le fonctionnement numérique de la Région Bretagne.

La DNSI

Région Bretagne, 283 Avenue du Général Patton, 35000

J'ai effectué mon alternance au sein de la **Région Bretagne**, une collectivité territoriale qui intervient dans de nombreux domaines publics tels que la gestion des lycées, les transports régionaux, le développement économique, l'aménagement du territoire et la transition numérique. Pour assurer le bon fonctionnement de l'ensemble de ses services, la Région s'appuie sur une infrastructure informatique centralisée et sécurisée, pilotée par la DNSI (Direction du Numérique et des Systèmes d'Information).

Au sein de la **DNSI**, j'ai intégré le pôle Réseau, une équipe composée de plusieurs ingénieurs réseaux spécialisés dans la gestion des infrastructures, la sécurité périmétrique, la connectivité des sites distants et la supervision des équipements. L'équipe est responsable du maintien en condition opérationnelle des équipements réseau (switchs, routeurs, firewalls), de la gestion des interconnexions entre les différents sites régionaux ainsi que de la sécurisation des flux de données. Elle intervient également sur les data centers hébergeant les services numérique délivrés aux usagers.

Mon intégration dans cette équipe m'a permis de découvrir un environnement professionnel structuré, avec des procédures précises, des contraintes fortes en matière de sécurité et une exigence élevée en termes de disponibilité des services. Travailler aux côtés d'ingénieurs réseaux m'a offert l'opportunité d'approfondir mes compétences techniques, de mieux comprendre les enjeux liés à la continuité de service et de participer à des projets concrets ayant un impact direct sur le fonctionnement numérique de la Région Bretagne.

DNSI

L’organisation de la DNSI

Région Bretagne, 283 Avenue du Général Patton, 35000

Remerciements

Je tiens à remercier sincèrement l'ensemble des personnes qui m'ont accompagné durant mon alternance au sein de la Région Bretagne.

Je remercie tout particulièrement mon maître d'apprentissage, ***Laurent Dumont****, pour sa confiance, sa disponibilité et la qualité de son encadrement. Ses conseils techniques et méthodologiques m'ont permis de progresser tout au long de mon année et de gagner en autonomie dans mes missions.*

Je souhaite également remercier les membres du service Réseau : ***Adrien Chabod****,* ***Danael Braux****,* ***Fabienne Molle****, ainsi que l'ensemble de l'équipe, pour leur accueil, leur patience et leur esprit d'équipe. Leur expertise et leur accompagnement m'ont permis de découvrir un environnement professionnel exigeant et formateur.*

Je remercie enfin l'ensemble des collaborateurs de la DNSI pour leur disponibilité et les échanges enrichissants que j'ai pu avoir tout au long de mon alternance.

Cette expérience au sein de la Région Bretagne a été très enrichissante, tant sur le plan technique que professionnel, et constitue une étape importante dans mon parcours en BTS SIO option SISR.

Activité 1

Intervention au data center de TDF à Cesson Sévigné

1.1 - Introduction & Préparation des opérations
1.2 - Protocole de redondance dans le datacenter
1.3 - Localisation et vérification des équipements
1.4 - Étiquetage de l’ensemble des nouveaux câbles d’alimentation
1.5 - Supervision de la redondance
1.6 - Conclusion de l’activité

Activité 1

Intervention au data center de TDF à Cesson Sévigné

1.1 - Introduction & Préparation des opérations

Dans le cadre de mon alternance au sein du service Réseau de la DNSI de la Région Bretagne, j'ai participé à une intervention au data center de la Région Bretagne, situé sur le site de TDF, à Cesson Sévigné.

L'entité de gestion du data-center à averti qu'une maintenance était planifiée concernant les réseaux éléctriques alimantants les baies de ces clients.

Chaque équipements placé au data-center profite de deux circuits d'alimentation élécctriques dinstinctes, avec un bloc d'alimentation dédié à chacune de ses voies éléctriques.

Afin de prévoir cette action de maintenance, une intervention sur site de la part de l'équipe réseau était nécessaire afin de s'assurer que chaque équipement était correctement raccordé aux différentes voies éléctriques. C'étaitt également l'occasion de déposer des câbles inutiliées et d'étiquetter correctement les câbles d'alimentation.

Cette intervention faisait suite à une information importante : une coupure programmée de la ligne électrique Voie A devait avoir lieu un mois plus tard. Cette opération technique impactait directement une des deux alimentations électriques du data center.

Il était donc indispensable de vérifier que tous les équipements institutionnels de la Région Bretagne étaient correctement configurés en redondance électrique. L'objectif était clair : garantir la continuité de service pendant la coupure et éviter toute interruption des systèmes informatiques régionaux.

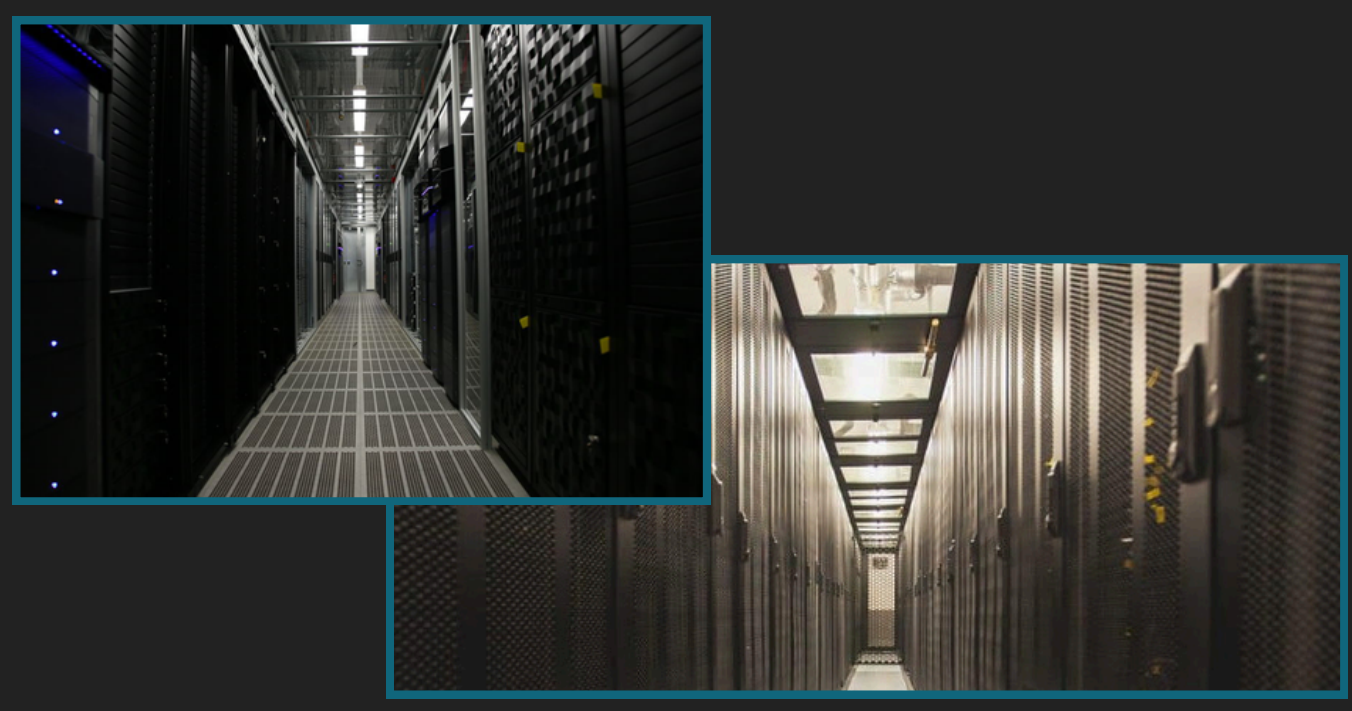
Avant le déplacement, nous avons préparé :

- La liste des équipements concernés (serveurs, équipements réseau, firewalls),
- Les plans d'implantation des baies,
- Le matériel nécessaire pour corriger d'éventuels mauvais branchements.

Nous avons également prévu des câbles d'alimentation identifiés par couleur :

- Voie A (Câble Rouge)
- Voie B (Câble bleu)

Ce choix permettait d'améliorer la lisibilité dans les baies, d'assurer une meilleure organisation et d'éviter toute confusion lors des vérifications. Cette préparation en amont était essentielle pour intervenir efficacement et limiter le temps passé sur site.



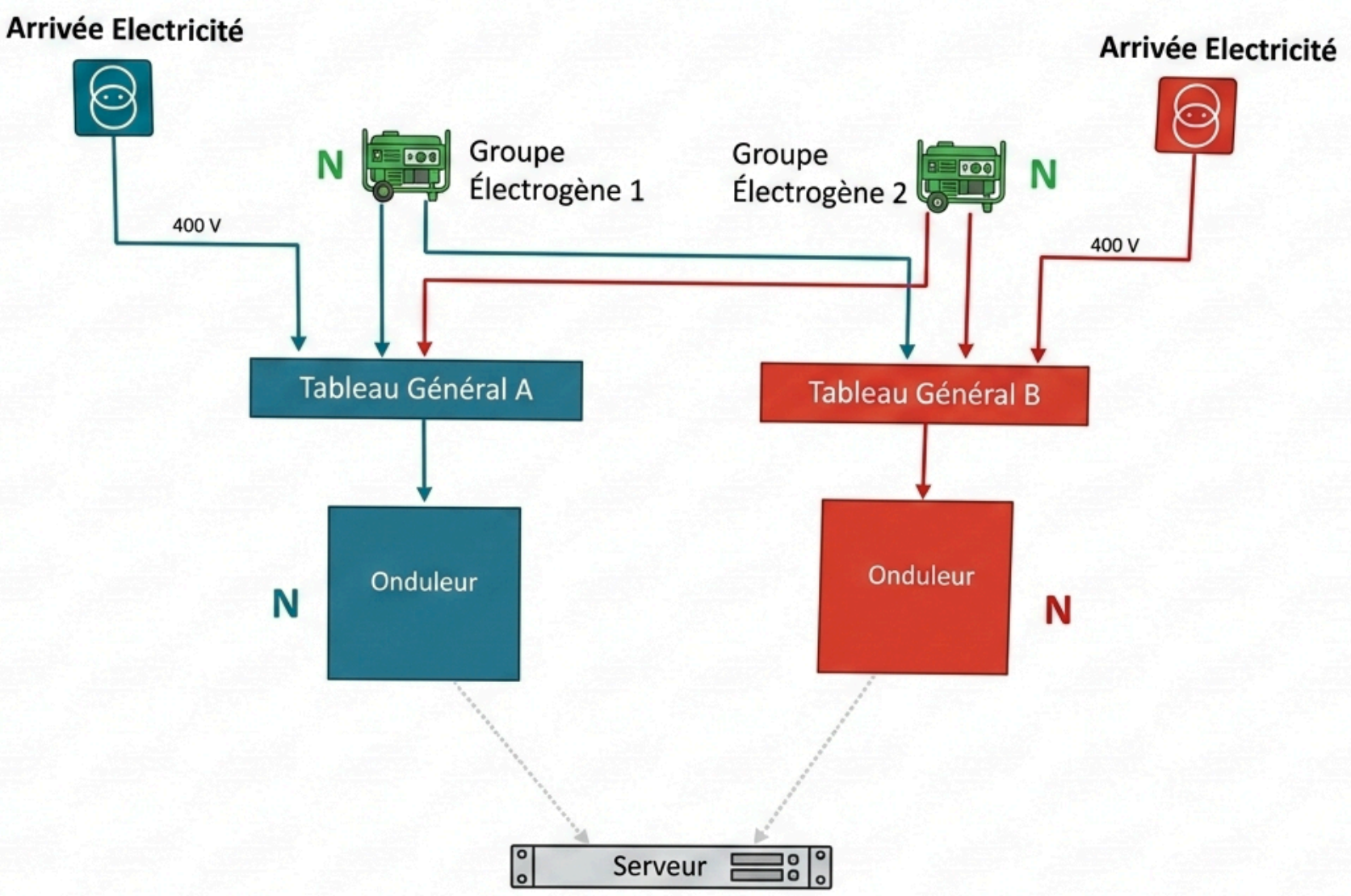
Activité 1.2

Intervention au data center de TDF à Cesson Sévigné

1.2 - Protocole de redondance dans le datacenter

Ce schéma représente le principe de double alimentation électrique dans un data center. Deux arrivées électriques indépendantes alimentent chacune un tableau général distinct (Voie A et Voie B). Chaque voie peut être secourue par un groupe électrogène en cas de coupure du réseau principal, puis passe par un onduleur qui stabilise la tension et prend le relais instantanément en cas de coupure. Les serveurs sont équipés de deux alimentations, chacune branchée sur une voie différente.

Ainsi, si la Voie A est coupée (maintenance ou incident), la Voie B continue d'alimenter les équipements sans interruption de service, ce qui garantit la continuité d'activité.



Activité 1.3

Intervention au data center de TDF à Cesson Sévigné

1.3 - Localisation et vérification des équipements

Une fois arrivés au data center de TDF à Cesson-Sévigné, nous avons commencé par identifier précisément les baies hébergeant les équipements de la Région Bretagne.
À l'aide des plans d'implantation et du repérage des racks (numéro de baie, position en U), nous avons procédé à un contrôle systématique équipement par équipement. Cette étape était importante afin d'éviter toute confusion avec d'autres matériels présents dans le data center.

Pour chaque équipement (swicth, firewalls, serveurs), nous avons réalisé plusieurs vérifications :

- Identification visuelle du matériel (modèle, étiquette, numéro d'inventaire),
- Vérification du nombre d'alimentations physiques présentes,
- Contrôle du branchement de chaque alimentation,
- Identification des PDU utilisées,
- Vérification de la correspondance entre PDU et Voie électrique (A ou B).

Chaque baie dispose de deux circuits électriques distincts :

- Voie A (Câble Rouge)
- Voie B (Câble bleu)

Ces deux voies sont indépendantes et permettent d'assurer la continuité de service en cas de coupure de l'une d'elles. Il était donc indispensable que chaque équipement disposant de deux alimentations soit réparti correctement entre ces deux circuits.

Dans certains cas, nous avons constaté que :

- Les deux alimentations étaient branchées sur la même PDU,
- Les câbles ne permettaient pas d'identifier clairement la voie utilisée,
- Le repérage était ancien ou partiellement effacé.

Ces situations annulaient la redondance électrique et représentaient un risque important en vue de la coupure programmée de la Voie A.

J'ai donc participé au rebranchement des alimentations afin de répartir correctement les équipements entre les deux colonnes électriques du data center. Les câbles ont été organisés selon leur voie d'alimentation : rouge pour la Voie A et bleu pour la Voie B. Cette différenciation permet une identification rapide et évite toute confusion lors d'interventions ultérieures.

Activité 1.4

Intervention au data center de TDF à Cesson Sévigné

1.4 - Étiquetage de l'ensemble des nouveaux câbles d'alimentation

Dans le cadre de la réorganisation électrique des baies, j'ai participé à l'étiquetage de l'ensemble des nouveaux câbles d'alimentation que nous avons ajoutés lors de la mise en conformité de la redondance.

Pour cela, nous avons utilisé une étiqueteuse professionnelle de marque Brady Corporation, équipée de consommables spécialement adaptés au marquage des câbles. Ces étiquettes sont conçues pour résister à la chaleur, aux manipulations et aux contraintes d'un environnement de data center.

Chaque nouveau câble installé a été identifié de manière précise avec :

- Le nom de l'équipement concerné
- La voie électrique correspondante (Voie A ou Voie B)

Les étiquettes ont été positionnées de façon visible et uniforme, tout en respectant le passage des câbles dans la baie afin de conserver une installation propre et structurée.
Ce travail permet une identification rapide des alimentations ajoutées et facilite les interventions futures, notamment en cas d'incident ou de maintenance électrique. Il contribue également à maintenir un niveau d'organisation conforme aux bonnes pratiques en environnement data center.

Activité 1.5

Intervention au data center de TDF à Cesson Sévigné

1.5 - Supervision de la redondance

Après la vérification physique des alimentations et la mise en conformité des branchements dans les baies du data center de TDF à Cesson-Sévigné, une phase de contrôle via nos outils de supervision a été réalisée.

L'objectif était de s'assurer que la redondance électrique n'était pas seulement correcte visuellement, mais également fonctionnelle du point de vue des systèmes.

Depuis les outils de supervision utilisés par la DNSI de la Région Bretagne, nous avons vérifié:

- L'état des alimentations remontées par les serveurs,
- Les alertes liées aux blocs d'alimentation (Power Supply Alert)
- Les éventuels messages d'erreur matériels
- La disponibilité des équipements réseau concernés.

Pour les équipements disposant d'interfaces de gestion, nous avons contrôlé que les deux alimentations étaient bien détectées comme actives et opérationnelles.

Cette étape nous a permis de confirmer que chaque équipement recevait bien une alimentation répartie sur deux circuits distincts, qu'aucune alerte critique n'était remontée dans nos outils et que l'ensemble des systèmes restait pleinement opérationnel. La supervision a donc permis de valider virtuellement les actions techniques réalisées sur site tout en assurant une visibilité continue sur l'état des équipements, notamment en prévision de la coupure programmée de la Voie A. Grâce à cette double vérification, à la fois physique et logicielle, nous avons pu sécuriser l'infrastructure avant l'intervention électrique prévue.

Activité 1.6

Intervention au data center de TDF à Cesson Sévigné

1.6 - Conclusion de l'activité

Cette intervention au data center de TDF à Cesson-Sévigné a été ma première expérience en environnement de data center professionnel. J'ai pu découvrir un cadre de travail très encadré, avec des règles strictes en matière d'accès, de sécurité et de manipulation des équipements.

Cette activité m'a permis de comprendre concrètement l'importance de la redondance électrique dans une infrastructure critique. J'ai pu participer aux vérifications physiques, au rebranchement des alimentations, à l'étiquetage des nouveaux câbles ainsi qu'au contrôle via les outils de supervision.

J'ai également pris conscience que l'organisation physique des baies (propreté, repérage, différenciation des voies A et B) joue un rôle essentiel en cas d'incident. Une infrastructure bien organisée facilite les interventions et réduit les risques d'erreur.

Cette première expérience en data center m'a permis de développer ma rigueur, mon sens de l'observation et ma compréhension des enjeux liés à la continuité de service pour la Région Bretagne.

Activité 2

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.1 - Introduction de l'intervention
2.2 - Planification du plan et configuration logiciel
2.3 - Début de l'étude de couverture sur le site
2.4 - Génération du rapport d'étude
2.5 - Déploiement de bornes supplémentaires
2.6 - Enregistrement et vérification du bon fonctionnement sur Meraki Cloud
2.7 - Le Meraki Cloud
2.8 - Prise d'informations aux utilisateurs, une semaine après l'intervention
2.5 - Conclusion de l'activité

Activité 2.1

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.1 - Introduction de l'intervention

Dans le cadre de mon alternance au sein du service Réseau de la DNSI de la Région Bretagne, j'ai participé à une étude Wi-Fi réalisée dans deux bâtiments institutionnels : le site du Bon Pasteur, qui comprend notamment la salle de l'hémicycle, ainsi que l'Hôtel de Courcy, où se situe le bureau du Président de la Région Bretagne.

Ces bâtiments accueillent régulièrement des réunions et des activités nécessitant une connexion Wi-Fi stable et performante. Il était donc important de vérifier que la couverture sans fil était homogène, suffisante et capable de supporter plusieurs connexions simultanées sans dégradation du service.

Avant l'intervention, nous avons défini les objectifs principaux : contrôler la qualité du signal dans les différentes zones, identifier les éventuelles zones de faible couverture, analyser l'occupation des canaux et préparer, si nécessaire, un ajustement du positionnement des points d'accès.

Nous avons également vérifié qu'aucune réunion ou événement officiel n'était prévu lors de notre passage afin de ne pas perturber l'activité des lieux et de pouvoir réaliser les mesures dans de bonnes conditions.

Cette phase d'organisation était indispensable pour assurer une intervention structurée et adaptée aux contraintes de ces bâtiments sensibles.

Activité 2.2

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

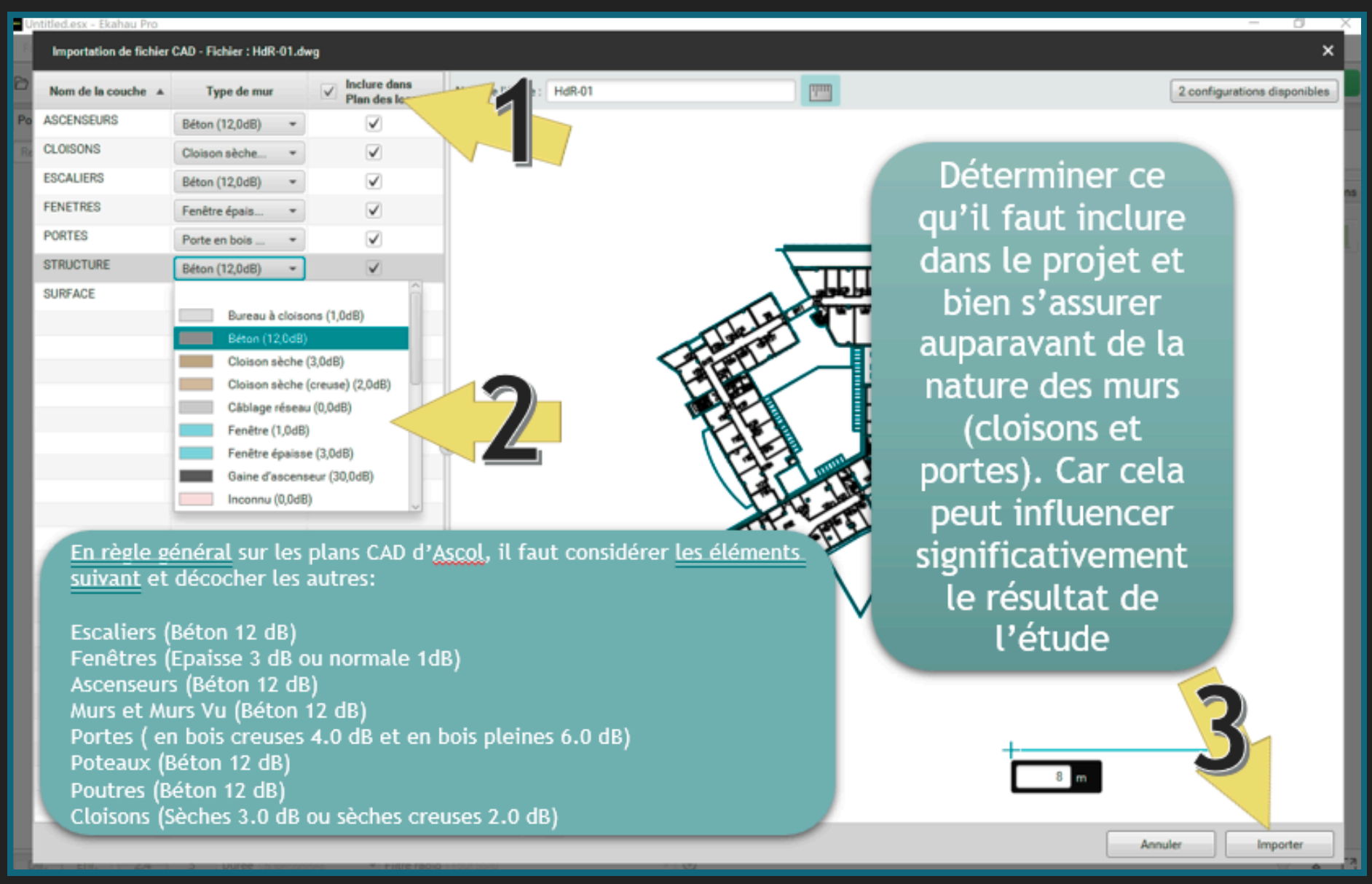
2.2 - Planification du plan et configuration logiciel

Dans un premier temps, il est indispensable de configurer à l'avance le plan du bâtiment dans le logiciel. Il faut indiquer précisément la composition des murs afin de simuler correctement l'atténuation des ondes Wi-Fi.

Le logiciel, utilisé est Ekahau Pro, qui est très complet : il demande également de renseigner les matériaux utilisés pour les portes, les vitres et l'ensemble des cloisons, car chaque matériau a un impact différent sur la propagation du signal.

Cette étape est relativement longue, car il est nécessaire de disposer de toutes les informations techniques pour construire un plan fidèle à la réalité. Une configuration imprécise pourrait fausser les résultats de l'étude.

Il est également important de mettre le plan à l'échelle dans le logiciel. Cette opération permet d'obtenir des mesures cohérentes lors des déplacements dans la salle et d'identifier correctement l'emplacement des bornes Wi-Fi, y compris celles installées au-dessus des faux plafonds.



Activité 2.3

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.3 - Début de l'étude de couverture sur le site

Une fois sur place, j'ai commencé l'étude de couverture Wi-Fi dans l'hémicycle ainsi que dans les différentes zones des bâtiments concernés. L'objectif était d'obtenir des mesures précises et représentatives de la réalité du terrain.

Pour cela, j'ai appliqué une méthode rigoureuse : je réalisais un point de mesure environ tous les trois pas. Cette technique permet d'obtenir un maillage dense et régulier des relevés, garantissant des calculs fiables et significatifs dans le logiciel Ekahau Pro.

J'ai longé les murs, parcouru les allées et traversé chaque pièce accessible afin d'éviter toute zone non analysée. L'objectif était d'obtenir une couverture complète, sans zone d'ombre ni espace non mesuré.

Ma mission durant cette phase était de m'assurer qu'aucune zone ne soit oubliée. Je devais vérifier que chaque partie du plan avait bien été couverte par des relevés et que l'ensemble des surfaces apparaissait correctement dans la cartographie finale. Cette méthode de déplacement structuré permet d'obtenir une cartographie précise de la couverture Wi-Fi et d'identifier de manière fiable les zones nécessitant une optimisation.

ekahau
WIRELESS DESIGN

Activité 2.4

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.4 - Génération du rapport d'étude

À l'issue des relevés réalisés avec Ekahau Pro, une cartographie de la couverture Wi-Fi a été générée pour la zone étudiée (correspondant à une aile du bâtiment).

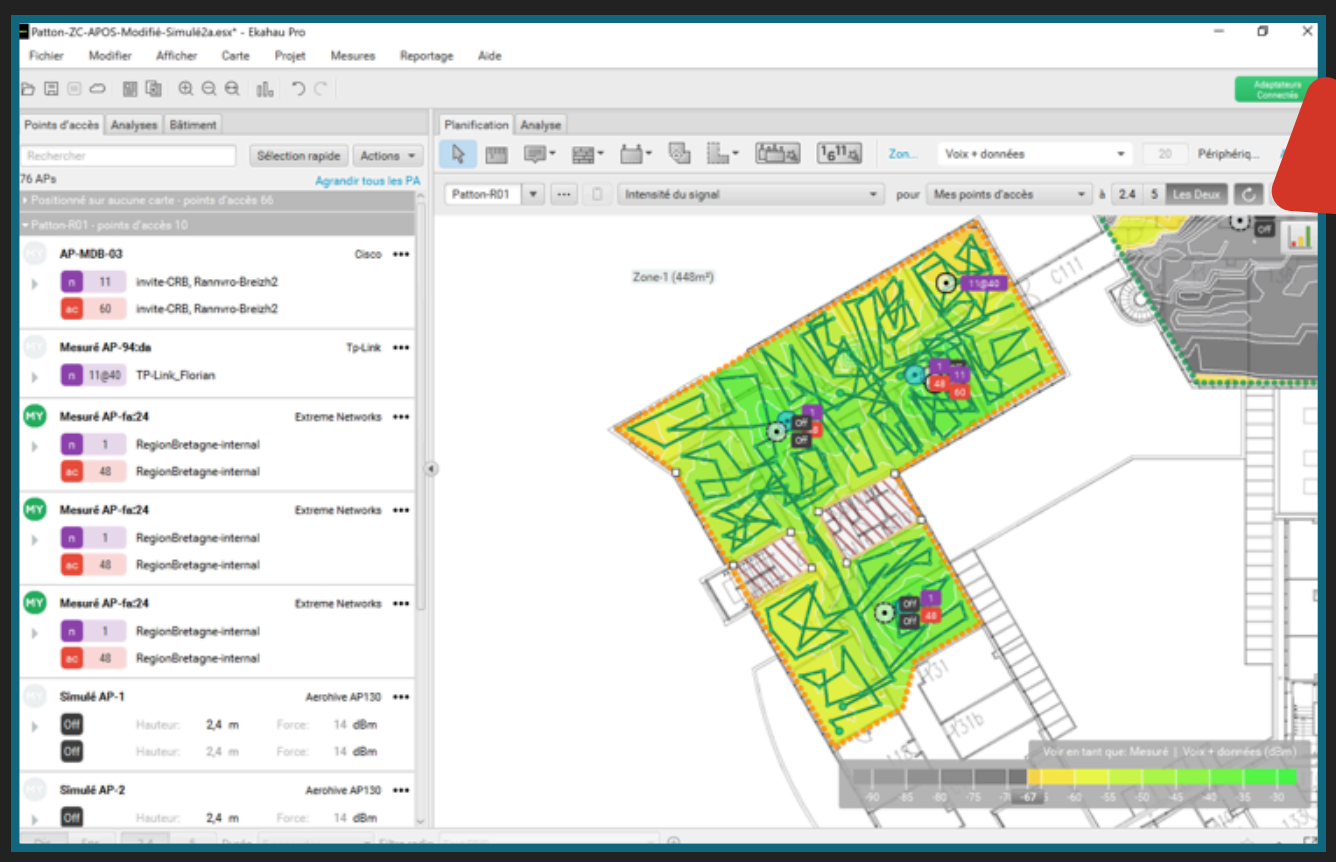
Le logiciel permet de visualiser la puissance du signal à l'aide d'un code couleur. Les zones en vert indiquent une couverture correcte, avec un signal suffisant pour un usage professionnel standard (navigation, messagerie, outils collaboratifs). Les zones en jaune ou orange traduisent une baisse de puissance du signal, ce qui peut entraîner une diminution des performances.

Lorsque certaines zones apparaissent en gris, cela signifie que la couverture Wi-Fi est insuffisante ou inexistante. Dans ce cas, le déploiement d'un nouveau point d'accès ou l'optimisation du positionnement et de la puissance des bornes existantes devient nécessaire. L'analyse ne se limite pas uniquement à la puissance du signal.

Elle permet également d'observer la continuité de la couverture, la cohérence entre les points d'accès et d'identifier d'éventuelles zones de rupture pouvant provoquer des pertes de connexion ou des difficultés lors des déplacements des utilisateurs.

Cette interprétation des résultats permet donc de prendre des décisions techniques concrètes : ajustement de puissance, modification des canaux ou ajout stratégique de bornes afin d'obtenir une couverture homogène et fiable sur l'ensemble de la zone étudiée.

Comme on peut l'observer dans cet extrait du rapport d'étude (qui comprend plusieurs dizaines de pages analysant en détail chaque fréquence et chaque signal) une zone grise apparaît dans la partie supérieure droite. Cette zone correspond à une couverture Wi-Fi insuffisante et devra être corrigée par le déploiement d'un point d'accès supplémentaire afin d'assurer une couverture homogène et stable.



Activité 2.5

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.5 - Déploiement de bornes supplémentaires

Suite aux résultats de l'étude Wi-Fi réalisée avec Ekahau Pro, certaines zones présentaient une couverture insuffisante. Le logiciel m'a permis d'identifier précisément les emplacements où l'ajout de nouvelles bornes était nécessaire afin d'améliorer la diffusion du signal dans ces zones.
J'ai donc participé au déploiement de points d'accès Cisco Meraki MR36 dans les emplacements indiqués par l'étude. Ces bornes ont été installées de manière à compléter la couverture existante et à assurer un signal plus homogène dans les différentes pièces du bâtiment.

Les bornes ont été raccordées au réseau grâce à la technologie Power over Ethernet (PoE) présente sur le commutateur, ce qui permet de les alimenter directement via le câble réseau, simplifiant ainsi l'installation et évitant l'ajout d'une alimentation électrique supplémentaire.

Après leur raccordement physique, il a été nécessaire de configurer les ports du switch pour renseigner les deux VLAN indispensables au fonctionnement des bornes. Le serveur DHCP a également été mis à jour afin de réserver une adresse IP correspondant à l'adresse MAC de chaque borne. De plus, une entrée RADIUS a été configurée sur un serveur Windows NPS afin d'assurer la sécurité de l'authentification des bornes sur le réseau.

Les VLAN définis ont été autorisés à communiquer sur la solution Cisco Meraki Cloud, ce qui permet d'intégrer automatiquement les nouvelles bornes au dashboard pour leur suivi et leur gestion.

Nous avons également choisi d'installer les bornes visibles sous le plafond plutôt que cachées dans le faux plafond, afin de faciliter les interventions futures, que ce soit pour la maintenance, les vérifications ou le remplacement éventuel d'un équipement.
Ce déploiement permet ainsi d'améliorer la couverture Wi-Fi globale et d'assurer une connexion plus stable et sécurisée pour les utilisateurs présents dans ces espaces.

Activité 2.6

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.6 - Enregistrement et vérification du bon fonctionnement sur Meraki Cloud

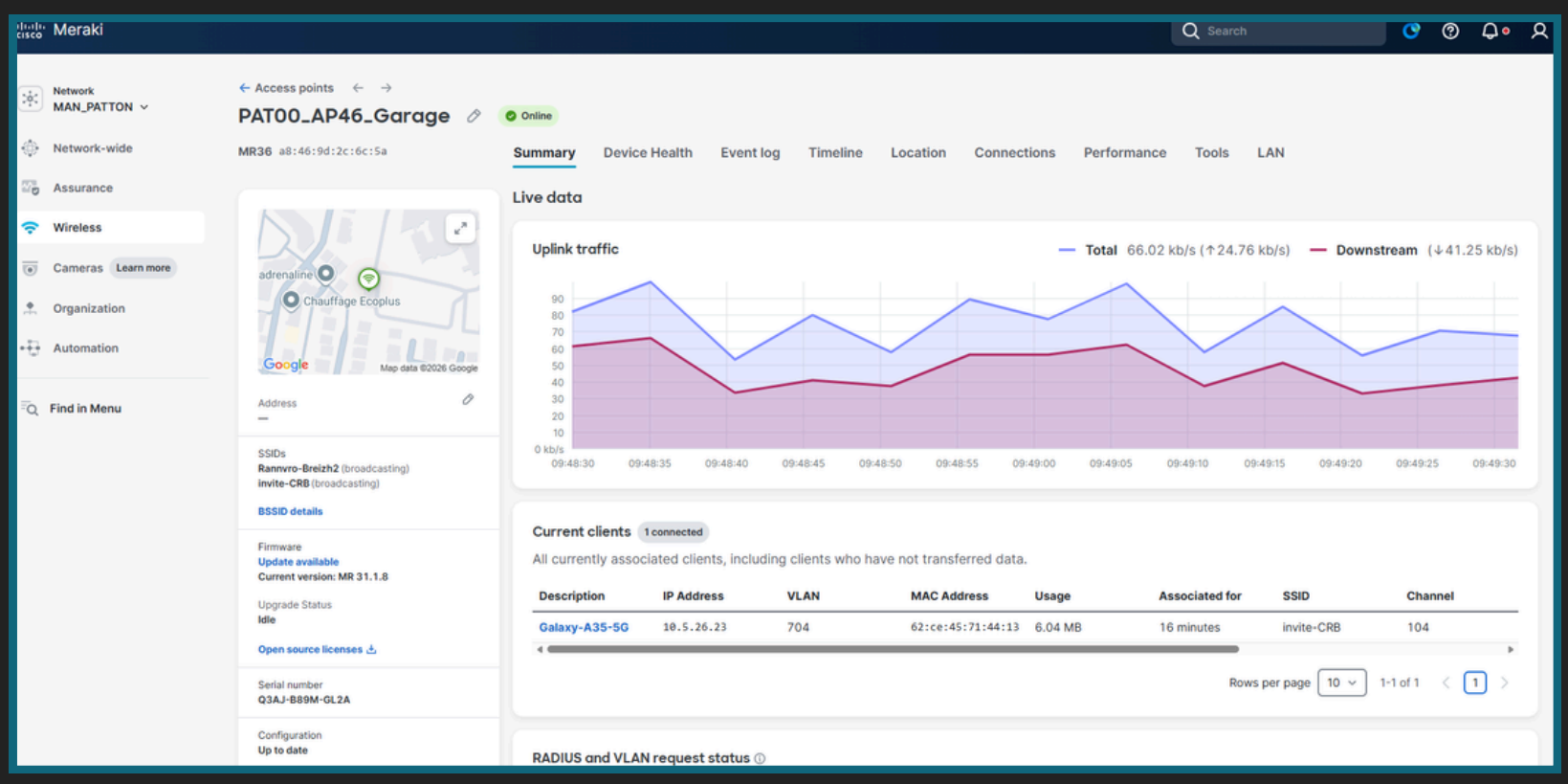
Une fois les bornes Wi-Fi installées et raccordées au réseau, j'ai procédé à leur enregistrement et à leur vérification dans l'interface de gestion Cisco Meraki Dashboard (Solution Cloud). Cette plateforme permet d'administrer à distance l'ensemble des équipements Cisco Meraki, comme les points d'accès.

Les bornes Cisco Meraki MR36 se connectent automatiquement au cloud dès qu'elles sont reliées au réseau et qu'elles disposent d'un accès à Internet. Une fois détectées dans le tableau de bord, j'ai pu les associer au réseau correspondant au bâtiment concerné. Cette étape permet de récupérer automatiquement la configuration Wi-Fi déjà définie par notre équipe, comme le nom des réseaux Wi-Fi (SSID), les paramètres de sécurité ou encore la gestion des canaux.

L'utilisation du cloud Meraki présente plusieurs avantages importants pour l'administration du réseau. Tout d'abord, il permet une gestion centralisée : tous les équipements peuvent être supervisés depuis une seule interface, sans avoir besoin de se connecter localement sur chaque borne. Cela facilite énormément le travail des équipes réseau, notamment lorsque les équipements sont répartis dans plusieurs bâtiments.

Enfin, le Meraki Cloud permet de simplifier la maintenance et les mises à jour. Les mises à jour logicielles peuvent être déployées automatiquement sur l'ensemble des bornes, ce qui permet de maintenir un niveau de sécurité et de performance optimal sans intervention physique sur les équipements.

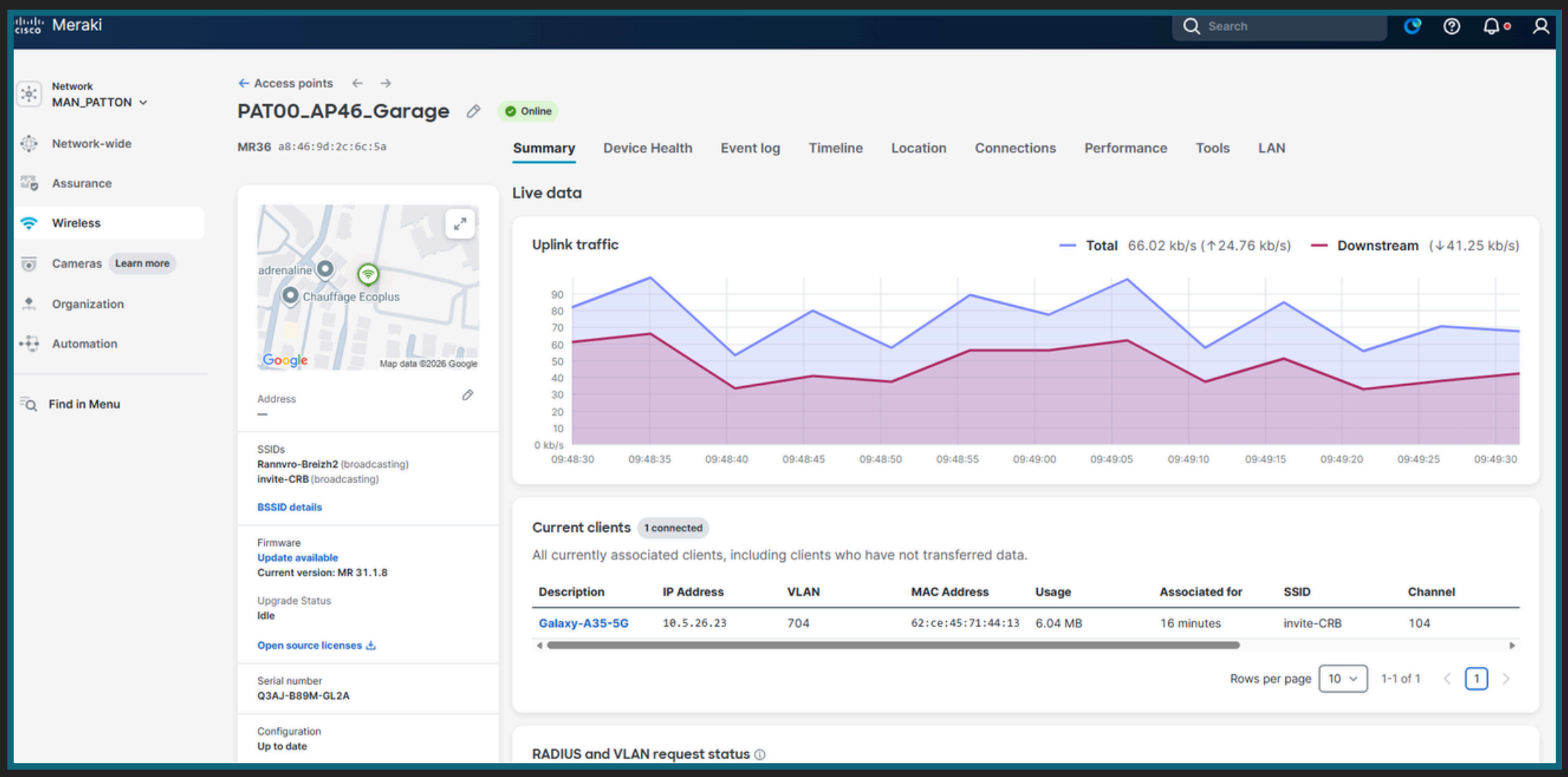
Cette phase de vérification était donc essentielle afin de confirmer que les nouvelles bornes étaient bien opérationnelles, correctement intégrées à l'infrastructure existante et pleinement supervisées par les outils de gestion du réseau.

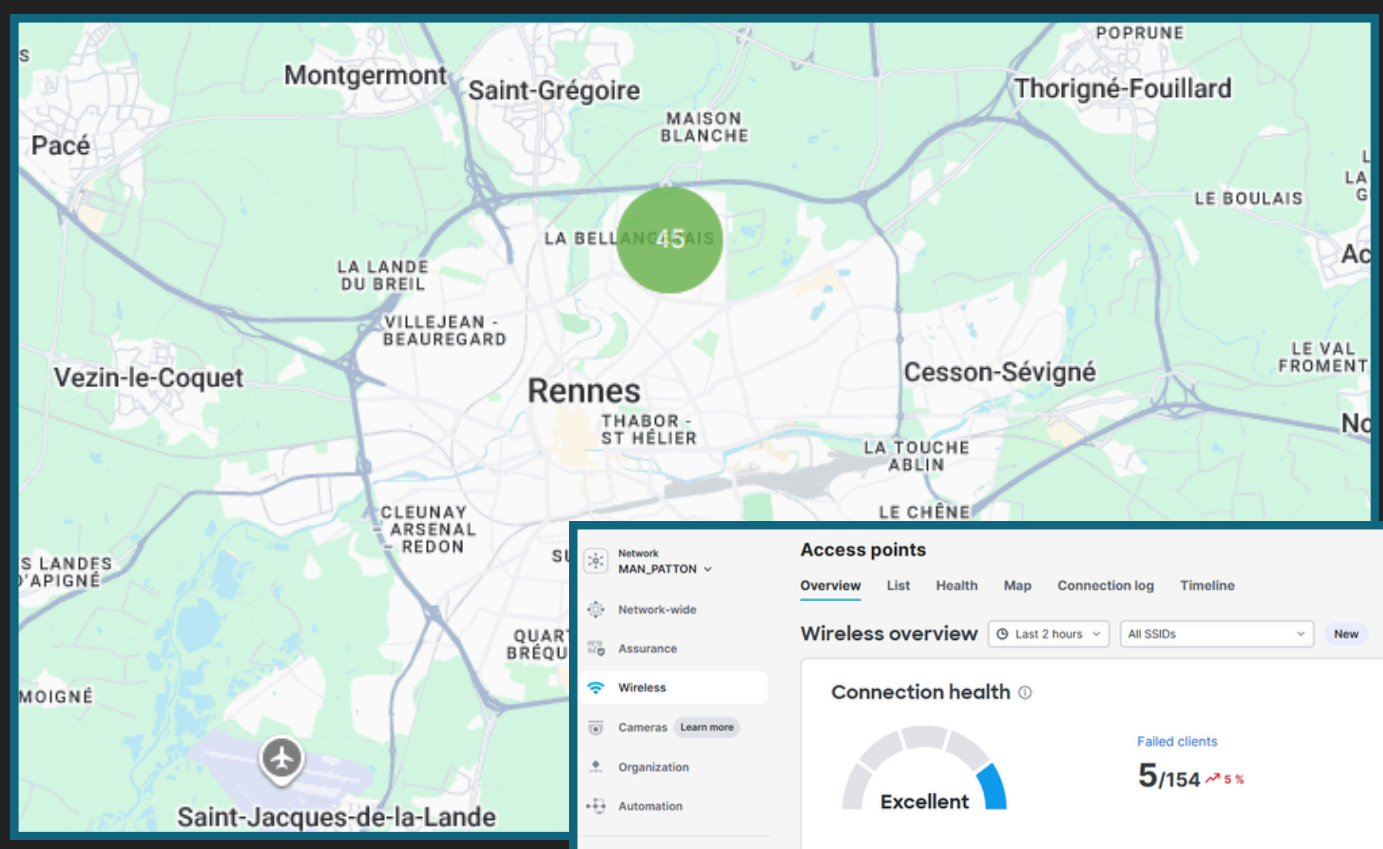


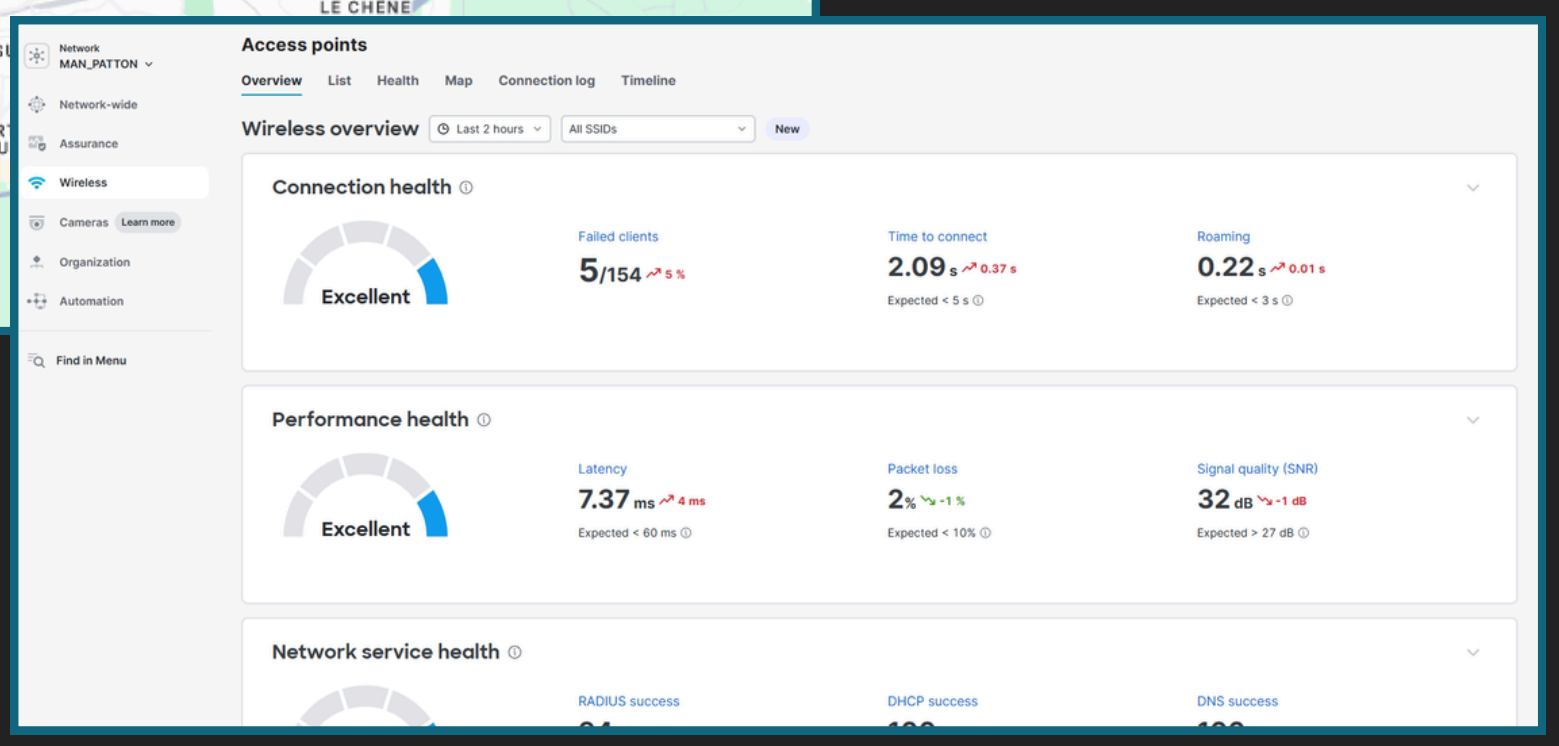
Activité 2.7

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.7 - Le Meraki Cloud







Activité 2.8

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.8 - Prise d'informations aux utilisateurs, une semaine après l'intervention

Une semaine après l'intervention et le déploiement des nouvelles bornes Wi-Fi, nous avons pris le temps de recueillir des informations auprès des utilisateurs présents dans les zones concernées. L'objectif était de vérifier si les améliorations apportées au réseau sans fil étaient bien perceptibles dans l'utilisation quotidienne.

Nous avons échangé avec plusieurs utilisateurs afin de savoir s'ils rencontraient encore des problèmes de connexion, des coupures ou des lenteurs sur le réseau Wi-Fi. Ces retours permettent de compléter les mesures techniques réalisées lors de l'étude et d'avoir une vision plus concrète de la qualité du réseau en situation réelle.

Les retours obtenus ont permis de confirmer que la couverture Wi-Fi était plus stable dans les zones où des points d'accès supplémentaires avaient été installés. Cette étape est importante, car elle permet de valider que les actions réalisées lors de l'étude et du déploiement répondent bien aux besoins des utilisateurs.

Activité 2.9

Déploiement de bornes et étude Wi-Fi à l'Hôtel de Courcy, l'hémicycle de la Région Bretagne

2.9 - Conclusion de l'activité

Cette intervention m'a permis de participer à une étude complète de couverture Wi-Fi dans des bâtiments importants de la Région Bretagne, notamment dans l'hémicycle situé dans le bâtiment Bon Pasteur et dans certaines zones de l'Hôtel de Courcy.

Grâce à l'utilisation du logiciel Ekahau Pro, j'ai pu découvrir la méthodologie nécessaire pour analyser la qualité d'un réseau sans fil et identifier les zones nécessitant des améliorations.

Au cours de cette activité, j'ai participé à plusieurs étapes du projet : la préparation de l'étude, la réalisation des mesures sur le terrain, l'analyse des résultats et le déploiement de nouvelles bornes Cisco Meraki MR36. J'ai pu mettre en oeuvre la configuration nécessaire au niveau des commutateurs et des entrées DHCP et RADIUS, comprendre l'impact des règles FIREWALL pour permettre les flux réseau d'atteindre le dashboard Meraki. J'ai également pu vérifier leur bon fonctionnement dans l'interface de gestion Cisco Meraki Dashboard, ce qui m'a permis de mieux comprendre l'intérêt de la supervision centralisée des équipements réseau.

Cette expérience m'a permis de comprendre concrètement comment une étude Wi-Fi est réalisée dans un environnement professionnel accueillant un grand nombre d'utilisateurs. J'ai également pu voir l'importance d'une bonne préparation, de mesures précises sur le terrain et de l'analyse des résultats afin de garantir une couverture réseau fiable.

Enfin, cette activité m'a permis de développer mes compétences dans le domaine des réseaux sans fil et de découvrir des outils professionnels utilisés par les ingénieurs réseau pour concevoir, déployer et optimiser les infrastructures Wi-Fi.

Activité 3

Projet "MAN" et segmentation de l'infrastructure

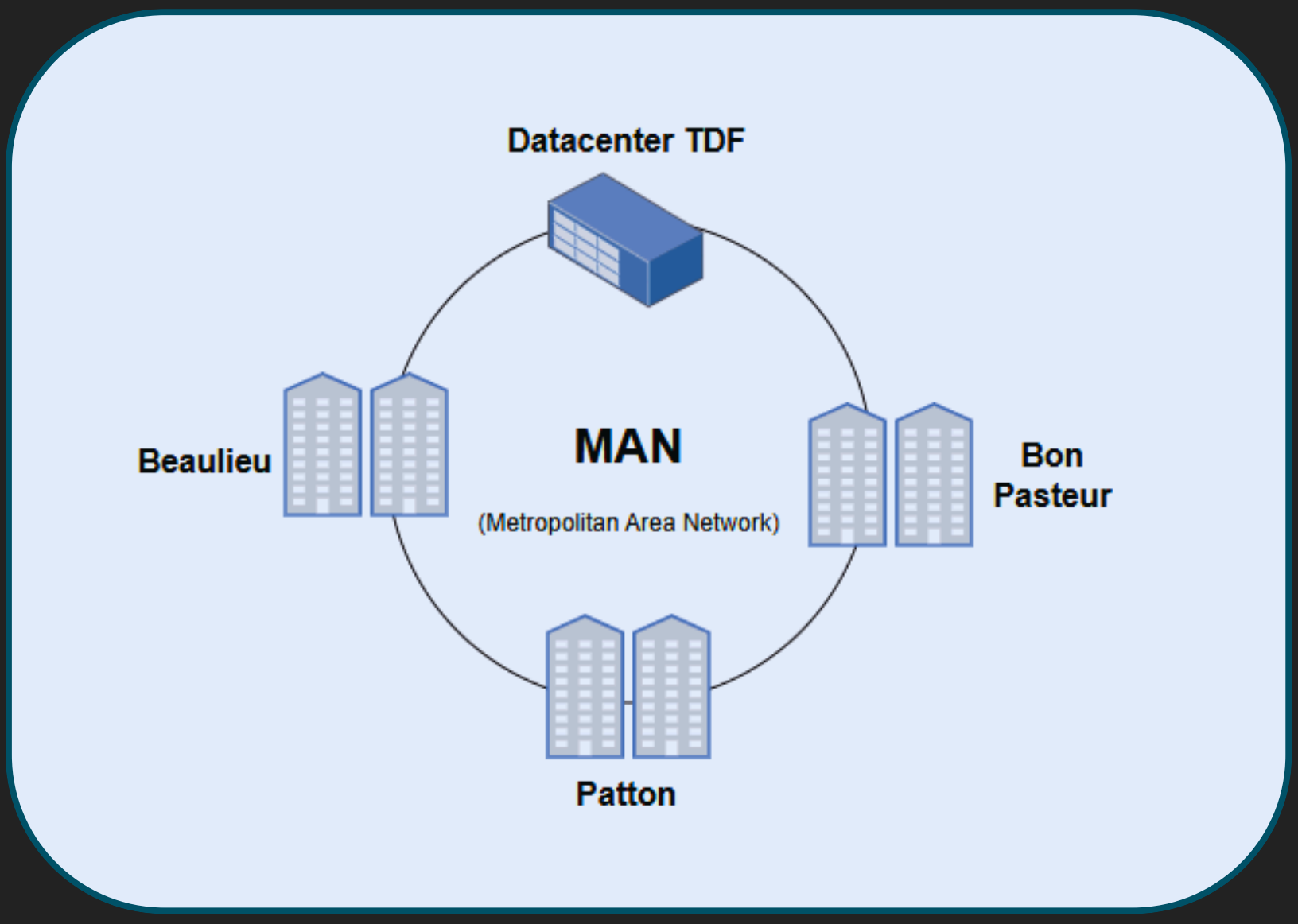
3.1 - Introduction à l’architecture “MAN”
3.2 - Migration des équipements dans les locaux techniques
3.3 - Migration progressif des utilisateurs dans les VLAN
3.4 - Retour des usagers
3.5 - Conclusion de l’activité.

Activité 3.1

Projet "MAN" et segmentation de l'infrastructure

3.1 - Introduction au projet “MAN”

Le projet **MAN** (Metropolitan Area Network) consiste à mettre en place un réseau en fibre noire reliant les différents sites importants de la métropole rennaise. Cette infrastructure est fournie par l’organisme FOR (Fibre Optique Rennaise), et repose sur une topologie en anneau. Ce type d’architecture permet d’assurer une continuité de service, car en cas de coupure sur un lien, le trafic peut passer dans l’autre sens.



La fibre noire arrive directement dans les bâtiments de la **Région Bretagne**, où elle est ensuite redistribuée sous forme de réseau en étoile vers les différents étages et équipements internes.

Ce projet a également été l’occasion de moderniser l’infrastructure réseau en remplaçant les anciens commutateurs Cisco par du matériel Hewlett Packard Enterprise, dans le cadre d’un marché dédié. Cela permet d’avoir un réseau plus performant, plus fiable et plus homogène.

Enfin, un des objectifs importants du projet **MAN** est l’amélioration de la sécurité du réseau. Pour cela, une segmentation des VLAN a été mise en place dans les bâtiments, afin de séparer les différents usages : utilisateurs, Wi-Fi, imprimantes, visioconférence, etc. Cette organisation permet de mieux gérer les flux réseau et de renforcer la sécurité globale de l’infrastructure.

Ce projet d’envergure est déployé de manière progressive et a été initié par la Région Bretagne il y a environ deux ans.

Activité 3.1 (BIS)

Projet "MAN" et segmentation de l'infrastructure

3.1 (BIS) - Introduction au projet “MAN”

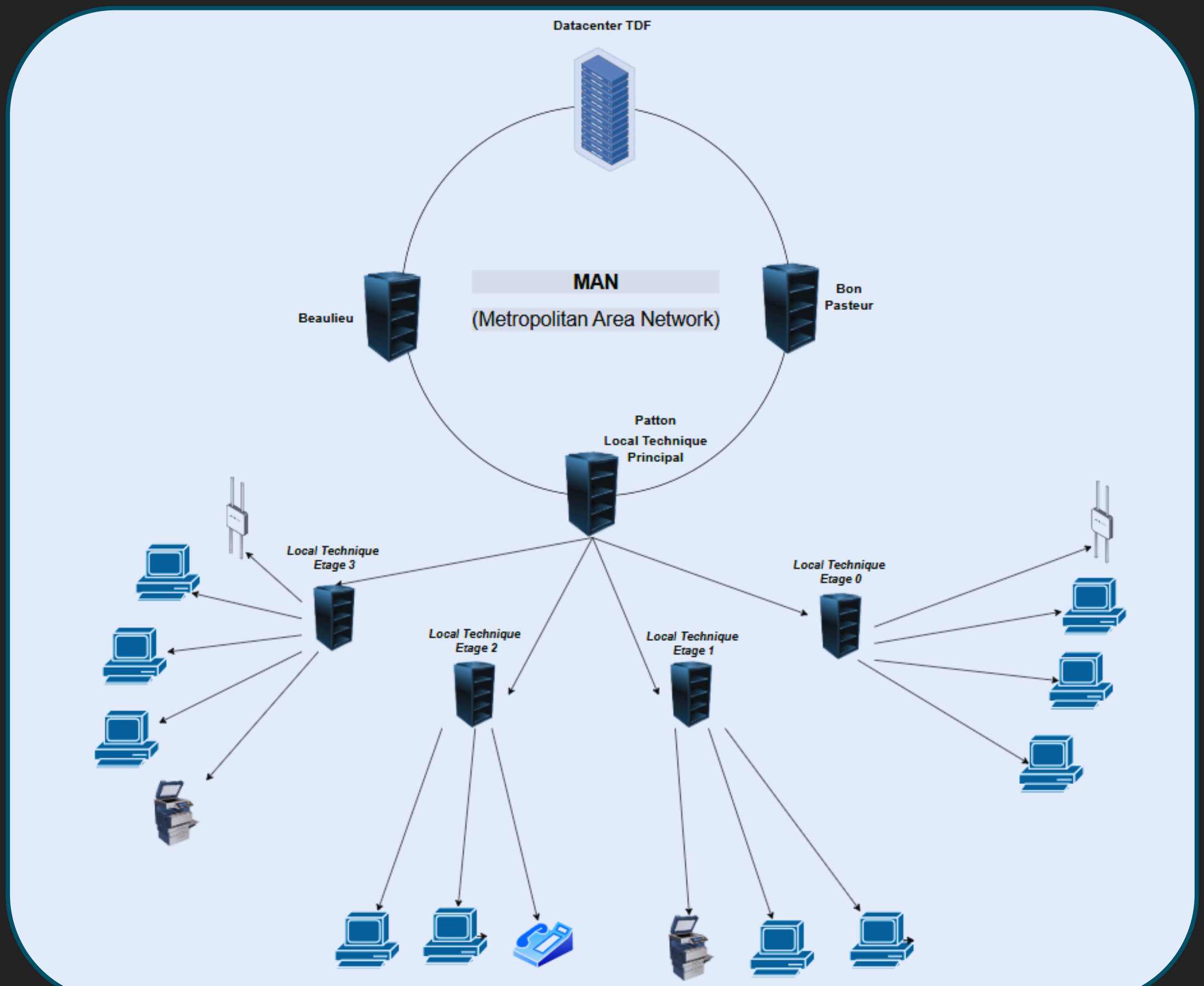


Schéma de l’arrivée de la fibre noire MAN dans le bâtiment de Patton et de sa propagation vers les locaux techniques des différents étages du site.

Activité 3.2

Projet "MAN" et segmentation de l'infrastructure

3.2 - Migration des équipements au sein des locaux techniques

Les switchs Cisco, devenus très anciens, présentaient des signes de fatigue avec une stabilité de plus en plus limitée. Leur remplacement était nécessaire pour garantir un réseau fiable.

Nous sommes passés à un nouvel environnement avec des switchs HPE 5710 pour raccorder les bâtiments à la boucle MAN, et des switchs HPE 5140 installés en stack pour l'ensemble des locaux techniques des bâtiments.

L'emploi des 5710 sur la boucle MAN à permis d'obtenir un débit de 10GB au lieu d'1GB. Le remplacement des rocades optiques entre les locaux techniques ainsi que l'emploi des commutateurs HPE 5140 à permis l'obtention du débit de 10GB sur l'ensemble des bâtiments..

Contrairement à l'ancienne architecture en cascade (où les switchs étaient reliés les uns à la suite des autres, ce qui n'était pas fiable), la nouvelle installation utilise un empilement de switchs avec des liaisons en fibre en **double attachement**. Cela permet d'assurer une meilleure redondance : si un lien tombe, le trafic peut continuer à circuler.

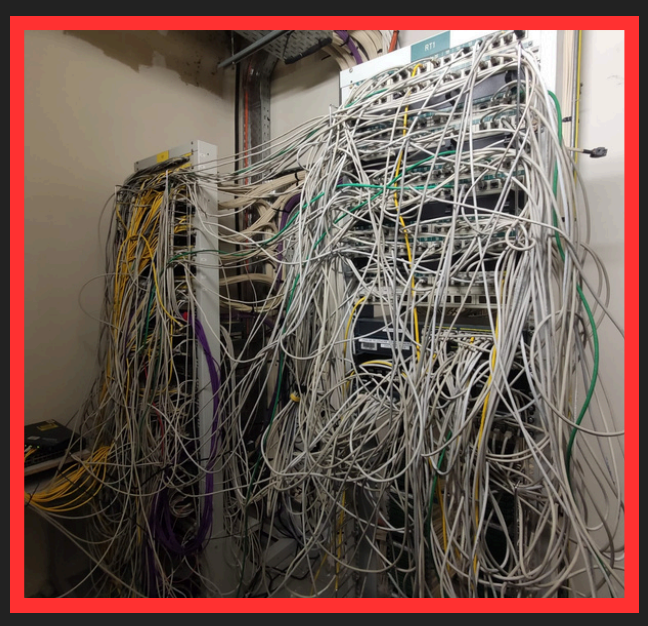
Un point important de l'intervention a été la qualité du brassage. Un câblage propre, organisé et bien étiqueté permet :

- **Une meilleure lisibilité des installations (gain de temps en maintenance).**
- **Une meilleure circulation de l'air dans les baies.**

Chaque baie a été soigneusement organisée pour obtenir un rendu propre et professionnel.
La mise en place d'un étage complet demandait plusieurs heures de travail, incluant le remplacement des équipements, le brassage et les vérifications. Cette opération a été réalisée sur les quatre étages du site de Patton.

Le résultat est une infrastructure beaucoup plus fiable, plus stable et plus performante, avec un réseau mieux organisé et plus simple à maintenir.

Avant



Après

Activité 3.3

Projet "MAN" et segmentation de l'infrastructure

3.3 - Nouvelle segmentation des VLAN

Après la migration initiale des équipements, nous avons mis en place une segmentation réseau par bâtiment et par type de service, afin d'optimiser l'organisation du réseau et la gestion des flux. Chaque bâtiment dispose désormais de VLAN dédiés :

Exemple de VLAN:

- VLAN 501 – DATA UTILISATEUR
- VLAN 504 – WIFI
- VLAN 502 – VISIO
- VLAN 503 – IMPRIMANTE

Chaque bâtiment dispose de tranches de VLAN spécifiques, permettant d'isoler les flux entre services et de limiter d'éventuelle compromissions.

Exemple de configuration d'un port de switch HPE, pour les utilisateurs, sur notre infrasturcture MAN:

```
interface GigabitEthernet1/0/5
 description
 port access vlan
 broadcast-suppression pps 2000
 multicast-suppression pps 15000
 stp root-protection
 stp edged-port
 stp port bpdu-protection enable
 undo lldp enable
 qos trust dscp
 ipv6 nd raguard role host
 dhcp snooping binding record
```

La migration vers cette architecture segmentée s'est faite progressivement, port par port, afin d'éviter toute interruption de service. Chaque équipement, postes, prises réseau ou bornes Wi-Fi, a été basculé vers son VLAN dédié en fonction du bâtiment et de son usage.
Un point clé de cette intervention a été la communication directe avec les utilisateurs.

Nous avons circulé dans les bureaux pour expliquer la démarche, les bénéfices de la segmentation et prévenir de courtes coupures éventuelles. Cette étape a permis de rassurer les utilisateurs et de favoriser leur adhésion, réduisant ainsi les risques d'incompréhension en cas de problème.

Grâce à cette approche, la transition vers la nouvelle architecture réseau s'est déroulée de manière fluide et maîtrisée, avec un réseau mieux structuré, plus performant et sécurisé, tout en maintenant la continuité de service.

Activité 3.4

Projet "MAN" et segmentation de l'infrastructure

3.4 - Retour des usagers

Après la mise en place de la nouvelle architecture réseau segmentée, nous avons évalué l'impact des changements réalisés sur la sécurité et la gestion des flux. L'un des objectifs principaux était de renforcer la cybersécurité et l'isolation des services.

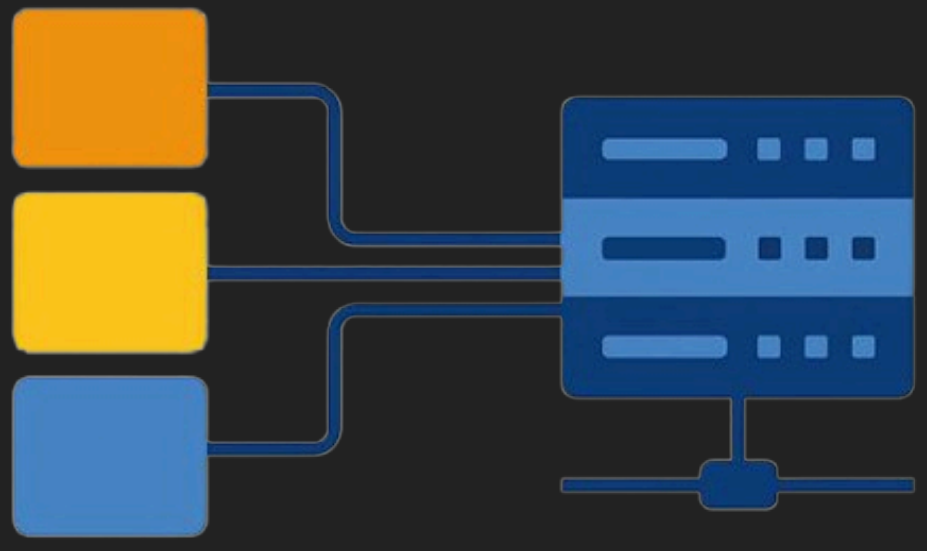
Grâce à la segmentation par VLAN, notamment VLAN 501 pour les postes utilisateurs (DATA), VLAN 504 pour le Wi-Fi, VLAN 502 pour la visioconférence et VLAN 503 pour les imprimantes, chaque type de trafic est désormais isolé et contrôlé. Chaque bâtiment dispose de tranches de VLAN spécifiques, ce qui limite la propagation des incidents et réduit les risques de compromission.

Cette segmentation offre plusieurs avantages sécuritaires :

- Isolation des flux pour éviter que des incidents sur un service n'impactent les autres.
- Contrôle d'accès renforcé grâce à la séparation stricte des VLAN.
- Surveillance simplifiée et détection plus rapide des anomalies ou tentatives d'intrusion.
- Limitation de la propagation des attaques entre bâtiments et services.

Les retours des utilisateurs ne montrent pas nécessairement de différence visible dans leur quotidien, mais pour la DNSI, la nouvelle segmentation par VLAN et par bâtiment offre une interprétation beaucoup plus rigoureuse du réseau. La logique est plus claire, la compréhension des flux plus simple et l'organisation des services plus structurée. Cette nouvelle tranche de VLAN permet de mieux analyser, contrôler et gérer le réseau, facilitant la planification et la réponse aux incidents.

VLAN
virtual local area network



Activité 3.5

Projet "MAN" et segmentation de l'infrastructure

3.5 - Conclusion de l’activité

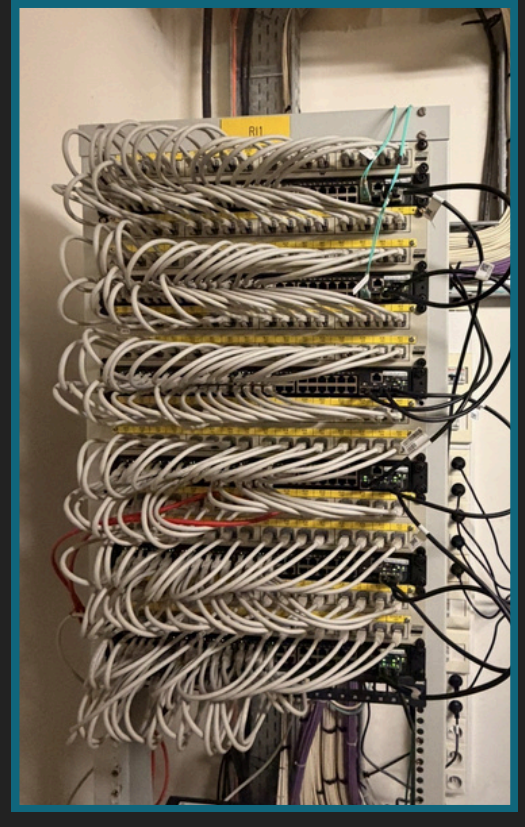
Cette activité m’a offert l’opportunité de participer concrètement au projet MAN de la Région Bretagne, en intervenant sur le remplacement des équipements et leur configuration, puis la migration progressive des utilisateurs et des différentes ressources dans les VLAN dédiés.

J’ai été impliqué dans la préparation des équipements déployés, incluant leur configuration et les vérifications nécessaires pour assurer un déploiement fiable. J’ai aidé à la dépose de l’ancien matériel, l’installation du nouveau, ainsi que la réalisation du brassage des baies.

Par ailleurs, j’ai contribué à la migration progressive des utilisateurs vers les nouveaux VLAN, en reconfigurant les ports et en assurant un suivi direct auprès des usagers. Cette expérience m’a montré l’importance d’une approche méthodique et progressive pour préserver la continuité de service tout en assurant une transition efficace vers la nouvelle architecture réseau.

Au-delà des aspects techniques, cette expérience m’a permis de développer ma rigueur, mon sens de l’organisation et ma capacité à gérer des interventions en conditions réelles. J’ai également pu acquérir une vision globale du fonctionnement d’un projet réseau de grande ampleur, en comprenant le rôle et les interactions de chaque intervenant, ainsi que l’importance de la planification et de la coordination.

Cette expérience a ainsi renforcé mes compétences techniques tout en consolidant ma capacité à analyser, anticiper et résoudre des problématiques réseau complexes, me préparant à des missions de plus grande responsabilité dans le domaine des infrastructures et de la cybersécurité.



Activité 4

Déploiement de LIBRENMS, Outil de supervision

4.1 - Introduction à LIBRENMS
4.2 - Déploiement en environnement de test
4.3 - Ajout des équipements en SNMP V3
4.4 - Ajout des équipements sur l'outil
4.5 - Scan de sécurité et déploiement en environnement de production.
4.6 - Conclusion de l'activité

Activité 4.1

Déploiement de LIBRENMS, Outil de supervision

4.1 - Introduction à LIBRENMS

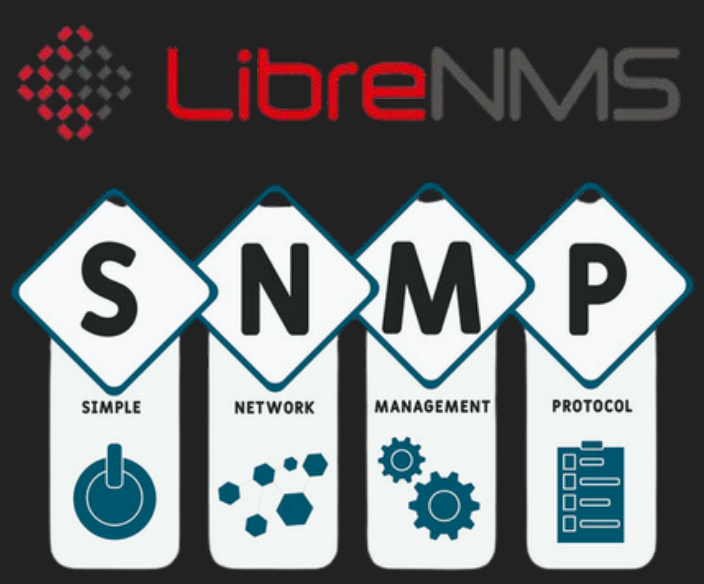
Dans le cadre de l'amélioration de la supervision du réseau, j'ai participé au déploiement de l'outil LibreNMS. Cet outil permet de surveiller en permanence l'état des équipements du réseau comme les routeurs, les switches, les serveurs ou encore les bornes Wi-Fi.

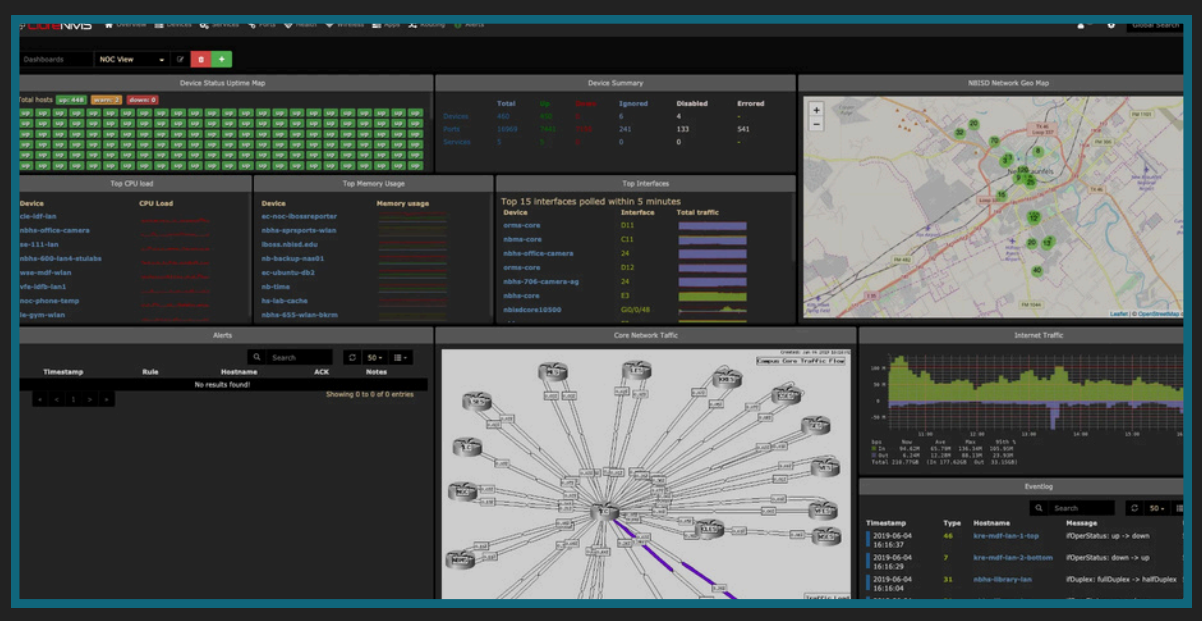
LibreNMS fonctionne principalement grâce au protocole SNMP, qui permet de récupérer de nombreuses informations directement depuis les équipements connectés au réseau. Ces informations sont ensuite centralisées dans une interface web qui affiche des graphiques, des statistiques et différents logs permettant de suivre l'activité du réseau.

Les logs et les données collectées sont très utiles pour comprendre ce qui se passe sur l'infrastructure. Par exemple, nous pouvons voir si un équipement redémarre, si une interface réseau rencontre des erreurs, ou encore si une liaison réseau est fortement utilisée. LibreNMS enregistre aussi l'état des équipements : s'ils sont en ligne, hors ligne ou s'ils ont rencontré une coupure.

Dans un cas concret, si des utilisateurs signalent un réseau lent dans un bâtiment, nous pouvons consulter les graphiques de trafic afin de vérifier si un lien réseau est saturé ou si un équipement consomme beaucoup de bande passante. De la même manière, si un switch devient inaccessible pendant quelques minutes, l'outil enregistre cet événement dans les logs avec l'heure précise de la coupure.

Les informations sont également conservées dans le temps, ce qui permet de revenir sur un incident pour analyser ce qui s'est passé. LibreNMS permet aussi de configurer des alertes : par exemple, nous pouvons être prévenus si un équipement tombe hors ligne, si la température d'un matériel devient trop élevée ou si l'utilisation d'un lien dépasse un certain seuil.
La mise en place d'un outil comme LibreNMS permet donc d'avoir une visibilité claire sur l'état du réseau et de faciliter l'identification des problèmes lorsqu'un incident se produit.





Activité 4.2

Déploiement de LIBRENMS, Outil de supervision

4.2 - Déploiement en environnement de test

Avant d'intégrer LibreNMS dans l'infrastructure principale, nous avons réalisé son déploiement dans un environnement de test. L'installation a été effectuée sur une machine fonctionnant sous Debian, ce qui permet d'avoir un système stable et largement utilisé pour l'hébergement de services réseau.

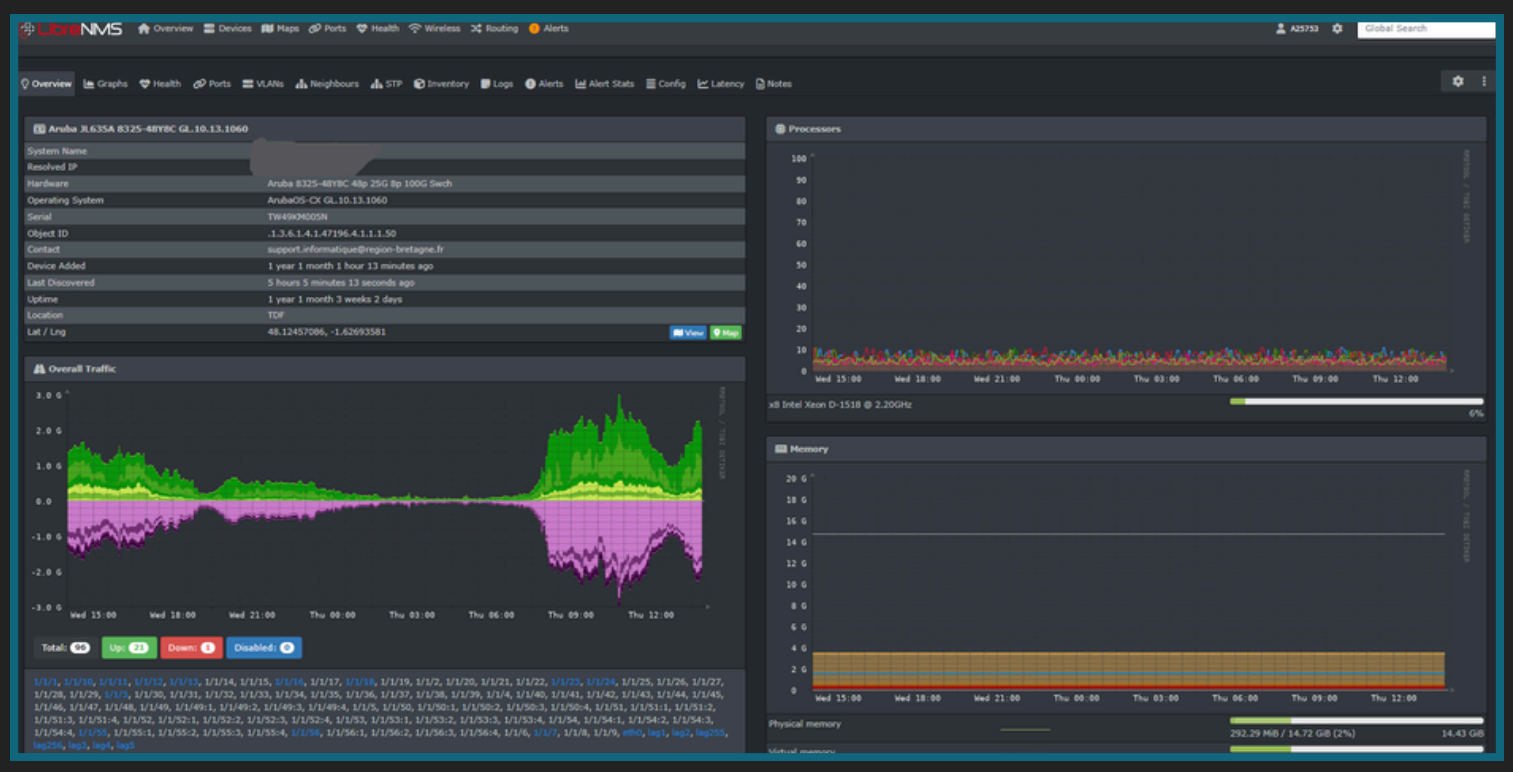
Cette première installation avait pour objectif de vérifier le bon fonctionnement de la plateforme et de tester ses différentes fonctionnalités avant une mise en production. Une fois l'installation terminée, nous avons commencé à ajouter quelques équipements de test dans la supervision afin de vérifier que la communication fonctionnait correctement via le protocole SNMP.

Cela nous a permis de confirmer que les informations remontaient correctement dans l'interface. Nous avons ensuite testé plusieurs fonctionnalités importantes de l'outil. Par exemple, nous avons vérifié l'affichage des graphiques de trafic sur les interfaces réseau, l'état des équipements (en ligne ou hors ligne) ainsi que la remontée des différentes informations techniques comme l'utilisation du processeur, de la mémoire ou de la bande passante.

Une partie du travail a également consisté à organiser le tableau de bord de supervision. Avec l'équipe, nous avons créé différents regroupements d'équipements afin de faciliter la lecture de l'interface. Cette organisation permet d'avoir une vue plus claire de l'infrastructure et de repérer plus rapidement un problème sur un équipement spécifique.

Nous avons aussi configuré les systèmes d'alerte, appelés triggers dans l'outil. Ces alertes permettent de définir à quel moment une notification doit être déclenchée. Par exemple, une alarme peut être configurée si un équipement devient inaccessible, si une interface réseau est saturée ou si certaines valeurs dépassent un seuil défini. L'objectif est d'être informé rapidement lorsqu'un problème apparaît sur le réseau.

Cette phase de test a permis de valider le fonctionnement général de LibreNMS et de préparer son utilisation dans un environnement réel. Elle nous a également permis de mieux comprendre les possibilités de l'outil et de mettre en place une organisation claire pour la supervision des équipements.



Activité 4.3

Déploiement de LIBRENMS, Outil de supervision

4.3 - Ajout des équipements en SNMP V3

Une fois LibreNMS correctement installé et configuré dans l'environnement de test, j'ai procédé à l'ajout des équipements réseau dans l'outil de supervision. Pour cela, j'ai utilisé le protocole SNMP en version SNMPv3, qui offre un niveau de sécurité plus élevé que les versions précédentes.

Dans le cadre de ce déploiement, j'ai créé un profil SNMPv3 standardisé destiné à être utilisé sur l'ensemble des équipements du réseau. L'objectif était de définir une configuration sécurisée et cohérente qui puisse ensuite être déployée facilement sur les routeurs, les switches et les autres équipements supervisés.

Contrairement aux versions plus anciennes du protocole, SNMPv3 permet d'intégrer des mécanismes d'authentification et de chiffrement. Les informations échangées entre les équipements et LibreNMS sont ainsi protégées contre l'écoute ou les accès non autorisés. Pour cela, j'ai configuré un utilisateur SNMP dédié à la supervision avec des identifiants spécifiques, ainsi que des paramètres de sécurité incluant l'authentification et le chiffrement des échanges.

Chaque équipement a donc reçu de nouveaux identifiants SNMP adaptés à cette configuration (voir configuration ci-dessous). Une fois ces paramètres appliqués sur les équipements et renseignés dans LibreNMS, l'outil a pu établir la communication et commencer à récupérer différentes informations techniques.

Après l'ajout d'un équipement, LibreNMS lance automatiquement une phase de découverte. Cette étape permet d'identifier les interfaces réseau, les capteurs disponibles, les statistiques de trafic ou encore certains services présents sur l'équipement. Les données récupérées sont ensuite utilisées pour générer des graphiques et alimenter les tableaux de bord de supervision.

Grâce à ce profil SNMPv3 sécurisé et standardisé, j'ai pu commencer à superviser plusieurs équipements et vérifier que les informations remontaient correctement dans l'interface. Cette configuration permet également de faciliter l'intégration de nouveaux équipements dans la supervision tout en conservant un niveau de sécurité adapté à l'infrastructure.

SNMP

SIMPLE NETWORK MANAGEMENT PROTOCOL

```
snmp-agent
snmp-agent local-engineid 800063A280303FBB0B739E00000001
snmp-agent community read snmpcrb acl 2001
snmp-agent sys-info contact support.informatique@region-bretagne.fr
snmp-agent sys-info location PATTON Garage [48.13470601471049, -1.6630889256350105]
snmp-agent sys-info version v2c v3
snmp-agent group v3 librenms
snmp-agent mib-view included iso-view iso
snmp-agent usm-user v3 librenms librenms cipher authentication-mode sha XXXXXXXXXXXXXX privacy-mode aes256
XXXXXX
```

Activité 4.4

Déploiement de LIBRENMS, Outil de Supervision

4.4 - Ajout des équipements sur l'outil

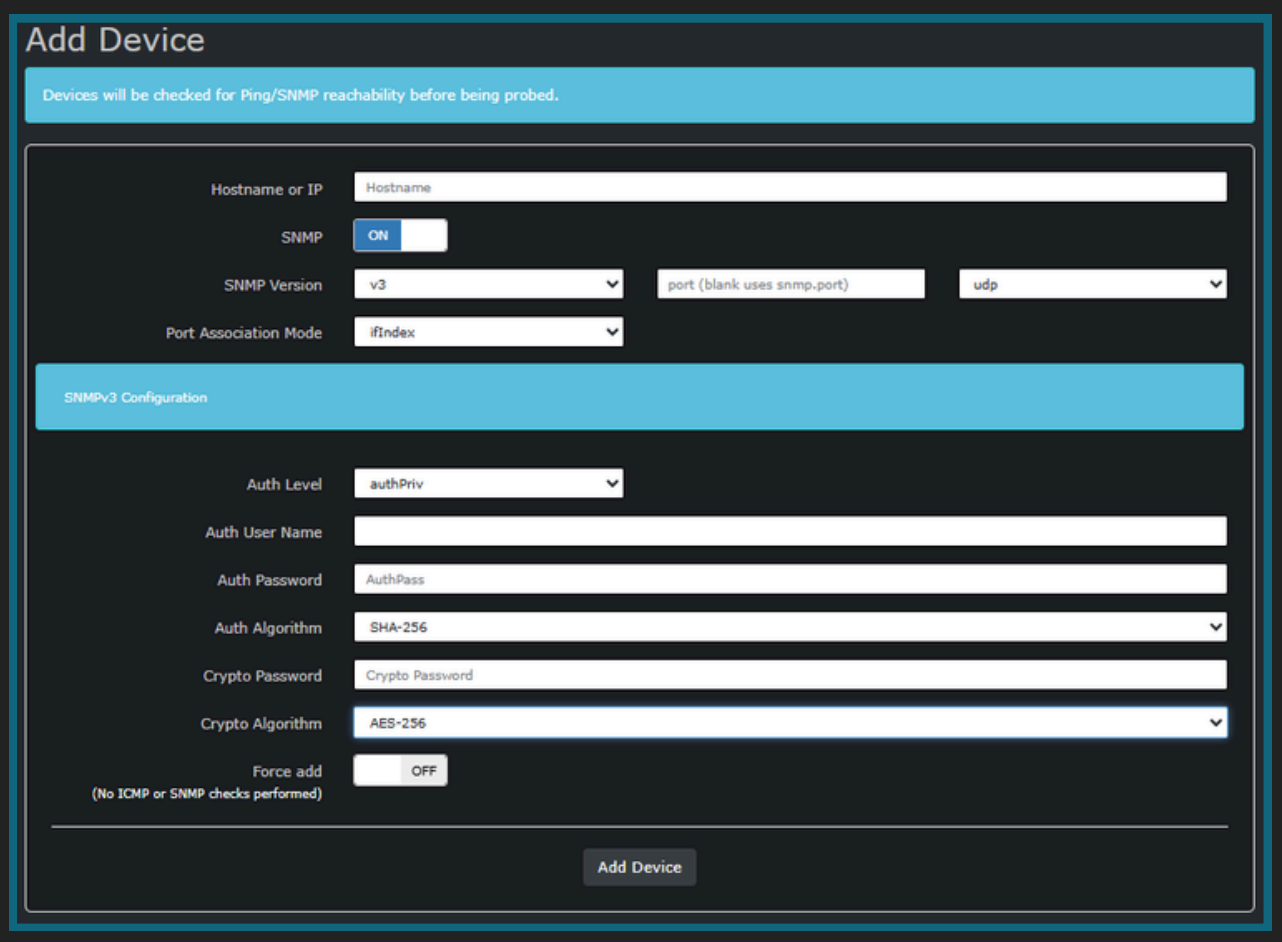
Une fois LibreNMS installé et sécurisé, j'ai procédé à l'ajout des équipements réseau directement dans l'interface de supervision. Cette opération se fait depuis la page Add Device, qui permet d'enregistrer un nouvel équipement à superviser.

Pour ajouter un équipement, j'ai d'abord renseigné son adresse IP ou son nom d'hôte afin que LibreNMS puisse le contacter sur le réseau. L'outil vérifie automatiquement si l'équipement répond au ping et au protocole SNMP avant de l'ajouter à la supervision.
J'ai ensuite configuré les paramètres SNMPv3 correspondant au profil sécurisé que j'avais précédemment mis en place. Cela incluait :

- Le niveau de sécurité authPriv, qui active à la fois l'authentification et le chiffrement,
- Le nom d'utilisateur SNMP dédié à la supervision,
- Le mot de passe d'authentification,
- L'algorithme d'authentification SHA-256,
- Le mot de passe de chiffrement,
- L'algorithme de chiffrement AES-256.

Ces paramètres permettent à LibreNMS de communiquer de manière sécurisée avec les équipements (et leurs paramètres vu précédemment) tout en protégeant les informations échangées. Une fois les informations renseignées, il suffit de valider l'ajout pour que l'outil commence automatiquement la découverte de l'équipement.

Cette étape est essentielle car elle permet d'intégrer progressivement les équipements dans la supervision. Une fois ajoutés, ils peuvent être surveillés en temps réel, ce qui facilite la détection d'anomalies et le diagnostic en cas de problème sur le réseau.



Activité 4.5

Déploiement de LIBRENMS, Outil de supervision

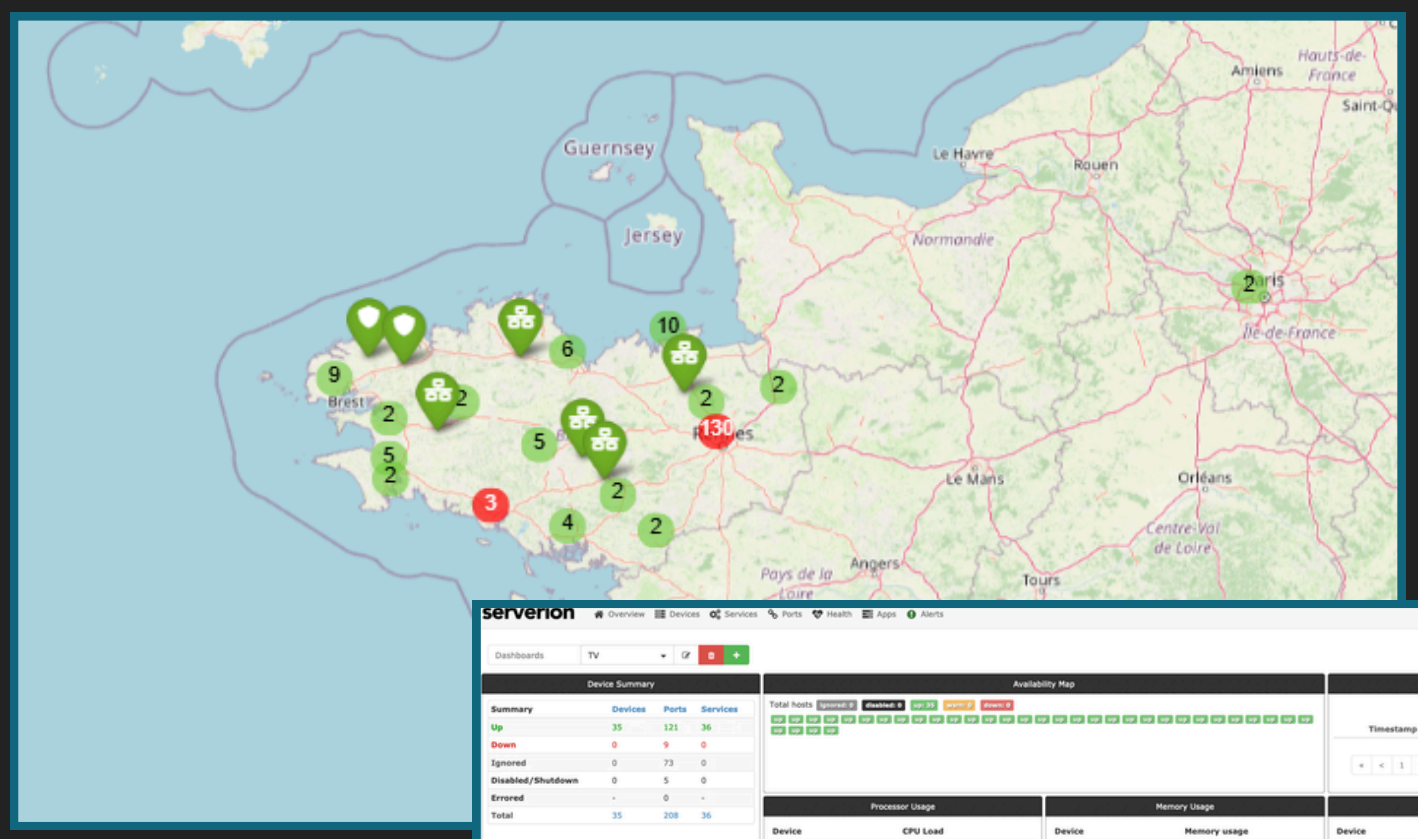
4.5 - Conclusion de l'activité

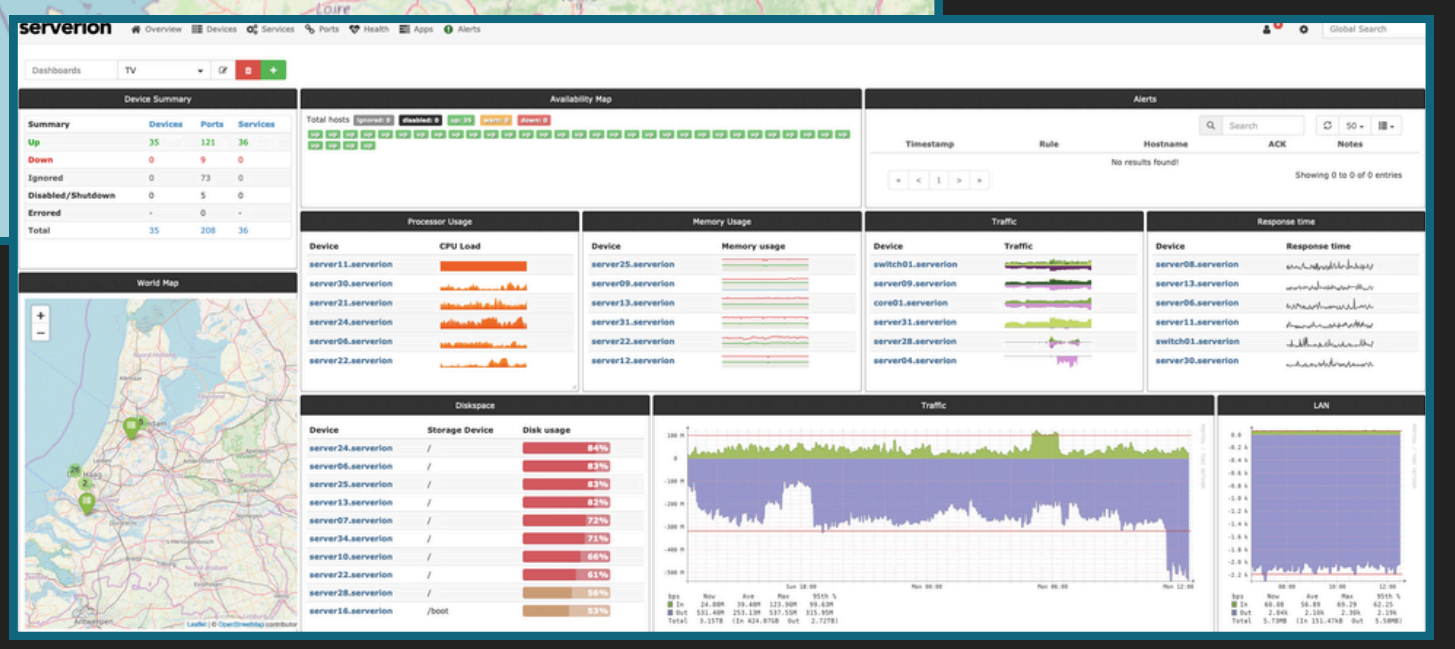
Cette activité m'a permis de participer au déploiement d'un outil de supervision réseau avec LibreNMS. J'ai pu suivre les différentes étapes nécessaires à sa mise en place, en commençant par l'installation sur un serveur sous Debian, puis par les tests dans un environnement dédié avant son déploiement en production.

Au cours de cette activité, j'ai également pu découvrir comment ajouter des équipements dans un outil de supervision grâce au protocole SNMP, en utilisant la version sécurisée SNMPv3. Cela m'a permis de mieux comprendre comment les informations techniques des équipements peuvent être récupérées et utilisées pour suivre l'état du réseau.

Cette expérience m'a aussi permis de voir l'importance d'un outil de supervision dans une infrastructure informatique. Grâce aux graphiques, aux logs et aux alertes, il est possible de surveiller en permanence le fonctionnement des équipements et de détecter rapidement un problème sur le réseau.

Enfin, cette activité m'a permis de développer mes compétences sur les systèmes de supervision réseau et l'organisation d'un outil de monitoring dans un environnement professionnel.





Activité 5

Déploiement d'HPE IMC sur le parc Institutionnel

5.1 - Étude du logiciel et projection du coût.
5.2 - Déploiement en environnement de test.
5.3 - Ajout des équipement en SNMP V3.
5.4 - Fonctionnement du protocol SNMP V3
5.5 - Réalisation des tests.
5.6 - Correction et identification de bugs.
5.7 - Présentation de l'environnement de test et validation du projet.
5.8 - Achat des licences et mise en relation avec le marché de la SPIE.
5.9 - Récéption des licences et installation en production.
5.10 - Déploiement officiel du logiciel et présentation à l'équipe.
5.11 - Conclusion de l'activité.

Activité 5.1

Déploiement d'HPE IMC sur le parc Institutionnel

5.1 - Etude du logiciel et projection du coût

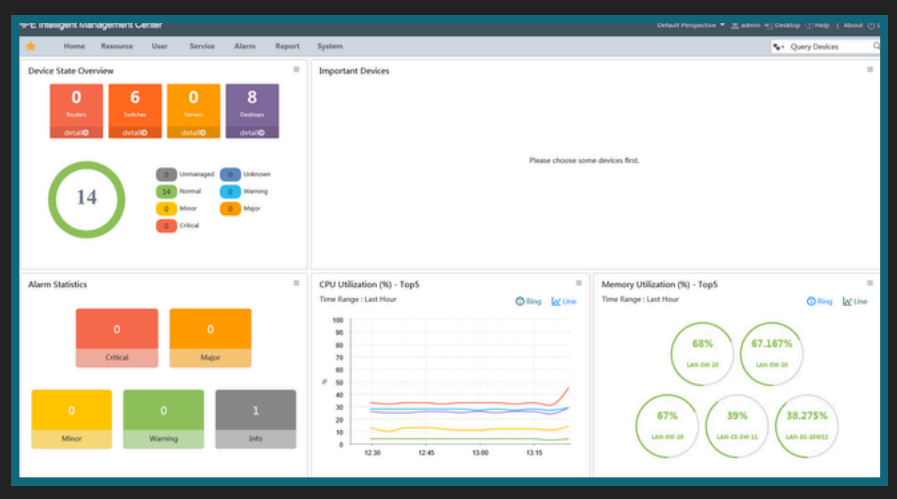
Dans le cadre du renouvellement du parc réseau de la Région Bretagne, les anciens équipements Cisco ont été progressivement remplacés par des switchs de la marque Hewlett Packard Enterprise. Cette évolution de l'infrastructure a conduit l'équipe réseau à réfléchir à la mise en place d'un outil permettant d'administrer et de superviser efficacement l'ensemble de ces nouveaux équipements. C'est dans ce contexte que j'ai été chargé d'étudier la solution HPE Intelligent Management Center, plus connue sous le nom d'HPE IMC.

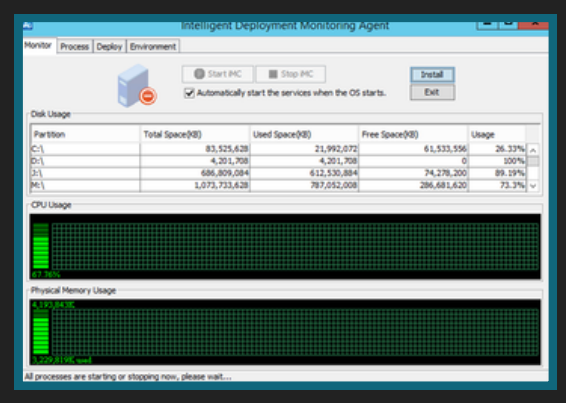
La première étape de mon travail a consisté à analyser les fonctionnalités du logiciel afin de déterminer s'il répondait aux besoins du réseau institutionnel. J'ai étudié les différentes possibilités offertes par l'outil, notamment la découverte automatique des équipements, la supervision des performances, la gestion centralisée des configurations, ainsi que la visualisation de la topologie du réseau. Ces fonctionnalités sont particulièrement utiles dans un environnement comprenant un grand nombre de switchs répartis sur plusieurs sites, car elles permettent d'avoir une vue claire et centralisée de l'infrastructure.

J'ai également évalué l'intérêt de cet outil dans le contexte du nouveau parc HPE. L'objectif était de vérifier que la solution permettrait de simplifier l'administration quotidienne du réseau, d'améliorer la supervision des équipements et de faciliter certaines opérations comme la sauvegarde automatique des configurations ou le déploiement de paramètres sur plusieurs switchs. L'étude a montré que l'intégration native avec les équipements HPE représentait un réel avantage pour la gestion du parc récemment installé.

En parallèle de l'étude technique, j'ai réalisé une projection du coût du projet. Cette étape impliquait l'analyse du modèle de licences proposé par HPE, qui dépend notamment du nombre d'équipements à superviser et des modules souhaités. J'ai recensé le nombre de switchs présents sur le réseau institutionnel afin d'estimer précisément les licences nécessaires. Cette estimation a ensuite été utilisée pour préparer une proposition budgétaire destinée à évaluer la faisabilité du projet.

Ce travail d'étude m'a permis de comprendre l'importance de la phase de préparation dans un projet d'infrastructure. Avant même le déploiement technique, il est essentiel d'analyser les besoins, d'évaluer les solutions existantes et d'estimer les coûts associés. Cette activité m'a appris à adopter une démarche structurée dans la conduite d'un projet informatique, en prenant en compte à la fois les aspects techniques et les contraintes budgétaires propres à une collectivité.





Activité 5.2

Déploiement d'HPE IMC sur le parc Institutionnel

5.2 - Déploiement en environnement de test

Après la phase d'étude du logiciel HPE Intelligent Management Center, l'étape suivante du projet a consisté à déployer la solution dans un environnement de test afin de vérifier son fonctionnement avant une éventuelle mise en production au sein du réseau de la Région Bretagne.

Pour réaliser ces tests, j'ai utilisé des licences d'évaluation fournies par Hewlett Packard Enterprise. Ces licences permettaient d'intégrer jusqu'à cinquante équipements dans la plateforme, ce qui était suffisant pour simuler une partie du parc réseau et analyser le comportement de l'outil dans des conditions proches de la réalité.

L'installation a été réalisée sur un serveur fonctionnant sous Windows Server. La base de données nécessaire au fonctionnement de l'application a été mise en place avec MySQL directement sur la même machine. Avant de procéder au déploiement, j'ai dû effectuer les démarches nécessaires auprès de l'équipe infrastructure afin de demander l'ouverture de la machine dans le réseau et l'autorisation des flux nécessaires au bon fonctionnement du logiciel. Cette étape était indispensable pour que le serveur puisse communiquer avec les équipements réseau présents dans l'infrastructure.

Une fois ces validations obtenues, j'ai procédé à l'installation du logiciel, à l'activation des licences de test et à la configuration initiale de la plateforme. La machine de test a été intégrée au réseau interne afin de permettre l'interaction avec nos équipements réels, notamment les switchs du parc HPE. Cela m'a permis d'ajouter plusieurs équipements dans la plateforme, de vérifier leur découverte automatique et d'observer la remontée des informations de supervision.

Ces tests avaient pour objectif de valider la compatibilité de la solution avec notre environnement, mais aussi d'évaluer les fonctionnalités de supervision, de cartographie réseau et de gestion centralisée des équipements. Le fait de travailler sur un environnement connecté au réseau réel a rendu les tests plus pertinents, car ils reproduisaient des situations proches de celles rencontrées en exploitation.

Cette étape m'a appris l'importance de tester une solution dans un environnement contrôlé avant toute mise en production. Elle m'a également permis de mieux comprendre les échanges entre un outil de gestion réseau et les équipements supervisés, tout en me familiarisant avec les procédures internes nécessaires pour intégrer une nouvelle machine dans une infrastructure existante.

Activité 5.3

Déploiement d'HPE IMC sur le parc Institutionnel

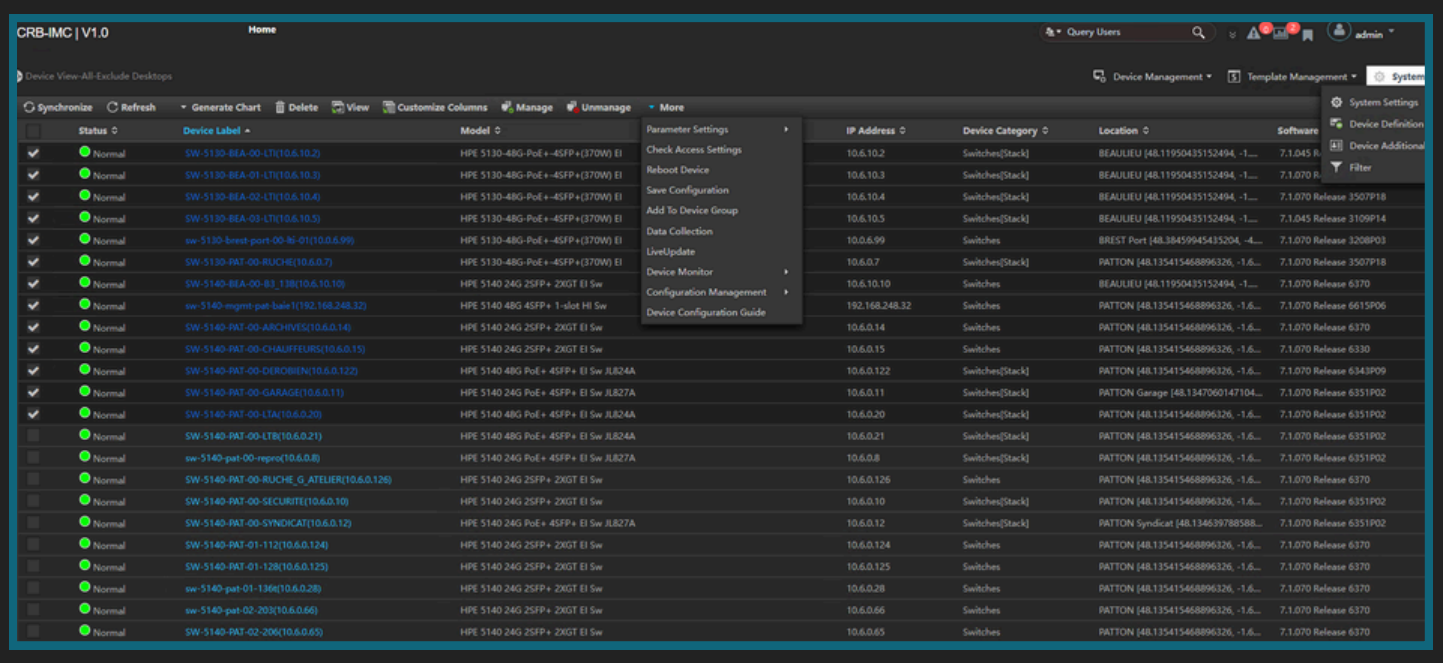
5.3 - Ajout des équipements en SNMP V3

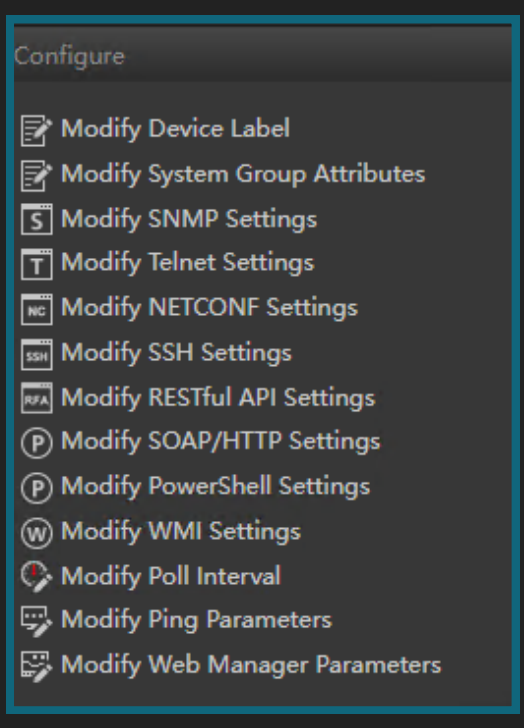
Une fois la plateforme HPE Intelligent Management Center installée en environnement de test, j'ai intégré les équipements du réseau afin de vérifier la supervision et l'administration centralisée des switchs Hewlett Packard Enterprise utilisés à la Région Bretagne.

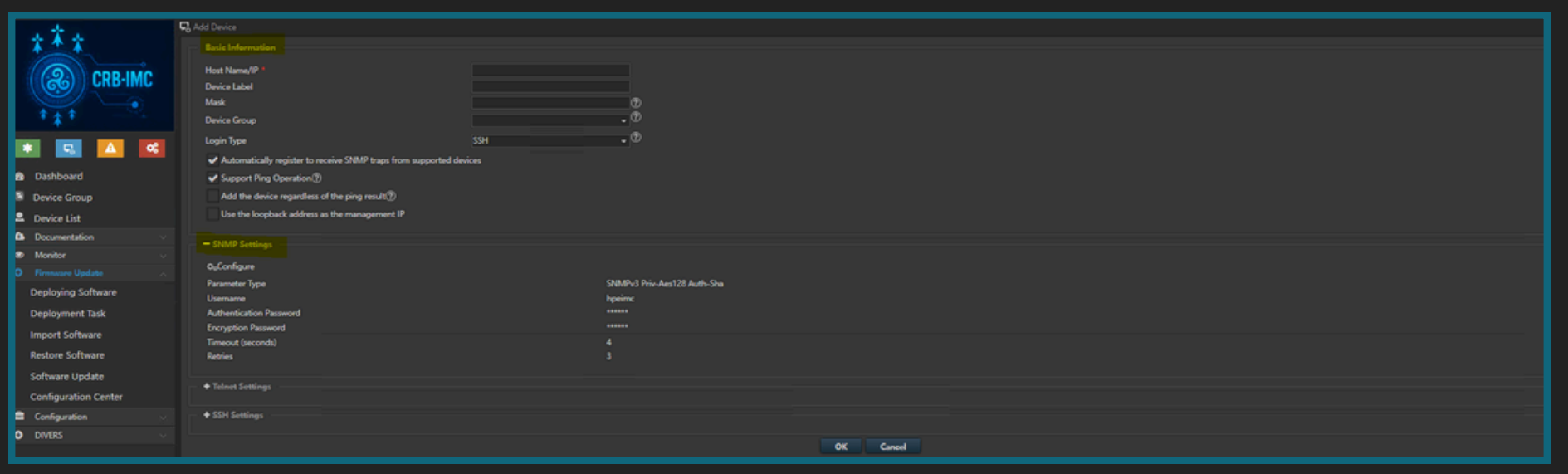
Pour cela, j'ai configuré l'ajout des équipements via le protocole SNMP en version 3. Ce protocole permet de récupérer des informations sur l'état des équipements, leurs interfaces et leur utilisation. Le choix du SNMPv3 est important car il apporte de la sécurité grâce à l'authentification et au chiffrement des échanges.

J'ai également mis en place des profils SNMP avec des droits en lecture et en écriture. Cela permet non seulement de superviser les équipements, mais aussi d'effectuer des actions directement depuis la plateforme, comme modifier des configurations ou intervenir sur plusieurs switchs en même temps.

Les tests ont permis de valider la communication entre la plateforme et les équipements, ainsi que le bon fonctionnement des fonctions d'administration. Cette étape m'a permis de mieux comprendre l'intérêt d'une gestion centralisée et le rôle du SNMP dans l'administration d'un réseau comportant de nombreux équipements.



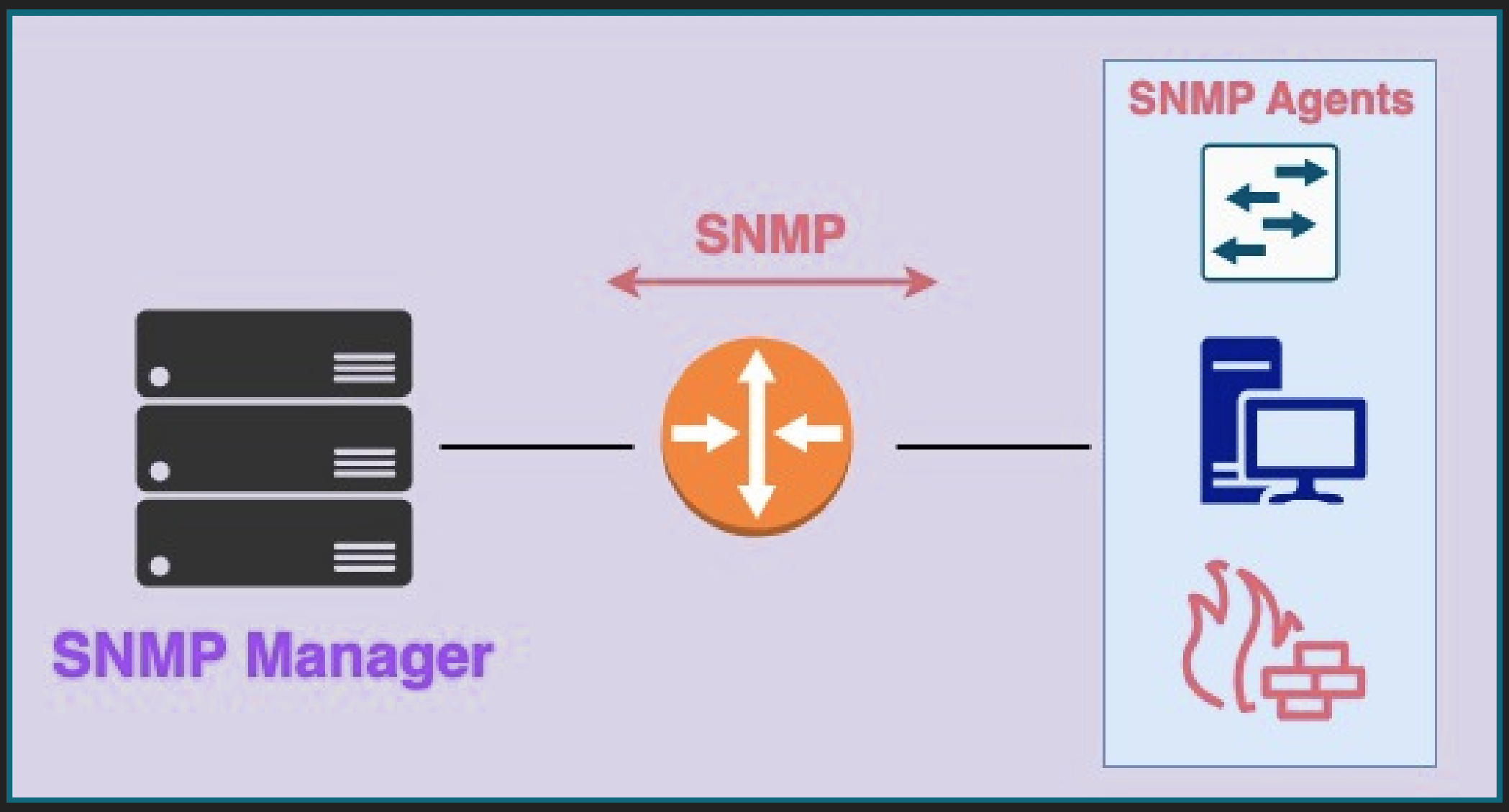




Activité 5.4

Déploiement d'HPE IMC sur le parc Institutionnel

5.4 - Fonctionnement du SNMP V3



HPE IMC utilise SNMP v3 pour surveiller et gérer les équipements réseau.

Chaque switch, routeur ou autre appareil doit avoir un agent SNMP activé avec un utilisateur SNMP v3 configuré (nom, mot de passe et niveaux de sécurité). IMC agit comme gestionnaire SNMP : il envoie des requêtes aux agents pour récupérer des informations via les MIB (trafic, interfaces, erreurs, etc.).

SNMP v3 assure que les échanges sont authentifiés et chiffrés, et IMC applique le contrôle d'accès pour savoir quels équipements et quelles données chaque utilisateur peut consulter. Ainsi, IMC centralise la supervision et la configuration des équipements de manière fiable et sécurisée.

Activité 5.5

Déploiement d'HPE IMC sur le parc Institutionnel

5.5 - Réalisation des tests

Après l'intégration des équipements dans la plateforme HPE Intelligent Management Center, j'ai réalisé une phase complète de tests afin d'évaluer la stabilité du logiciel et son impact sur les ressources du serveur. Cette étape était importante pour vérifier que l'outil pouvait être utilisé dans de bonnes conditions au sein du réseau de la Région Bretagne.

Lors de ces tests, j'ai analysé la consommation de ressources du serveur ainsi que le comportement des différents modules du logiciel. Certaines fonctions de sondes de supervision se sont révélées particulièrement gourmandes en ressources et peu utiles dans notre contexte, car une partie de ces informations était déjà collectée par l'outil de supervision LibreNMS, qui est déjà en place sur le réseau et qui remplit très bien ce rôle. Afin d'éviter une redondance inutile et d'optimiser les performances du serveur, j'ai donc désactivé certaines sondes qui n'apportaient pas de valeur supplémentaire pour notre exploitation.

Suite à ces analyses, nous avons fait le choix d'orienter l'utilisation de HPE IMC principalement vers l'administration centralisée des équipements plutôt que vers la supervision pure. L'outil est en effet particulièrement efficace pour effectuer des actions d'écriture sur les équipements réseau, ce qui représente un réel gain de temps dans la gestion d'un parc important de switchs.

Pour valider ces fonctionnalités, j'ai réalisé plusieurs tests concrets d'administration sur les équipements du parc Hewlett Packard Enterprise. J'ai notamment testé le déploiement de mises à jour de firmware sur certains équipements, la création et le déploiement d'ACL, la configuration de VLAN, ainsi que la modification de paramètres sur les ports des switchs. J'ai également réalisé des opérations plus simples mais essentielles pour l'exploitation quotidienne, comme le changement du nom des équipements ou la désactivation de ports inutilisés.

Ce travail m'a permis de comprendre l'importance de tester en profondeur un outil avant sa mise en production. Il m'a également appris à analyser les besoins réels d'une infrastructure afin d'adapter l'utilisation d'un logiciel à son contexte, plutôt que d'utiliser toutes ses fonctionnalités sans distinction. Cette démarche m'a aidé à développer une approche plus réfléchie dans le choix et l'exploitation des outils d'administration réseau.

Activité 5.6

Déploiement d'HPE IMC sur le parc Institutionnel

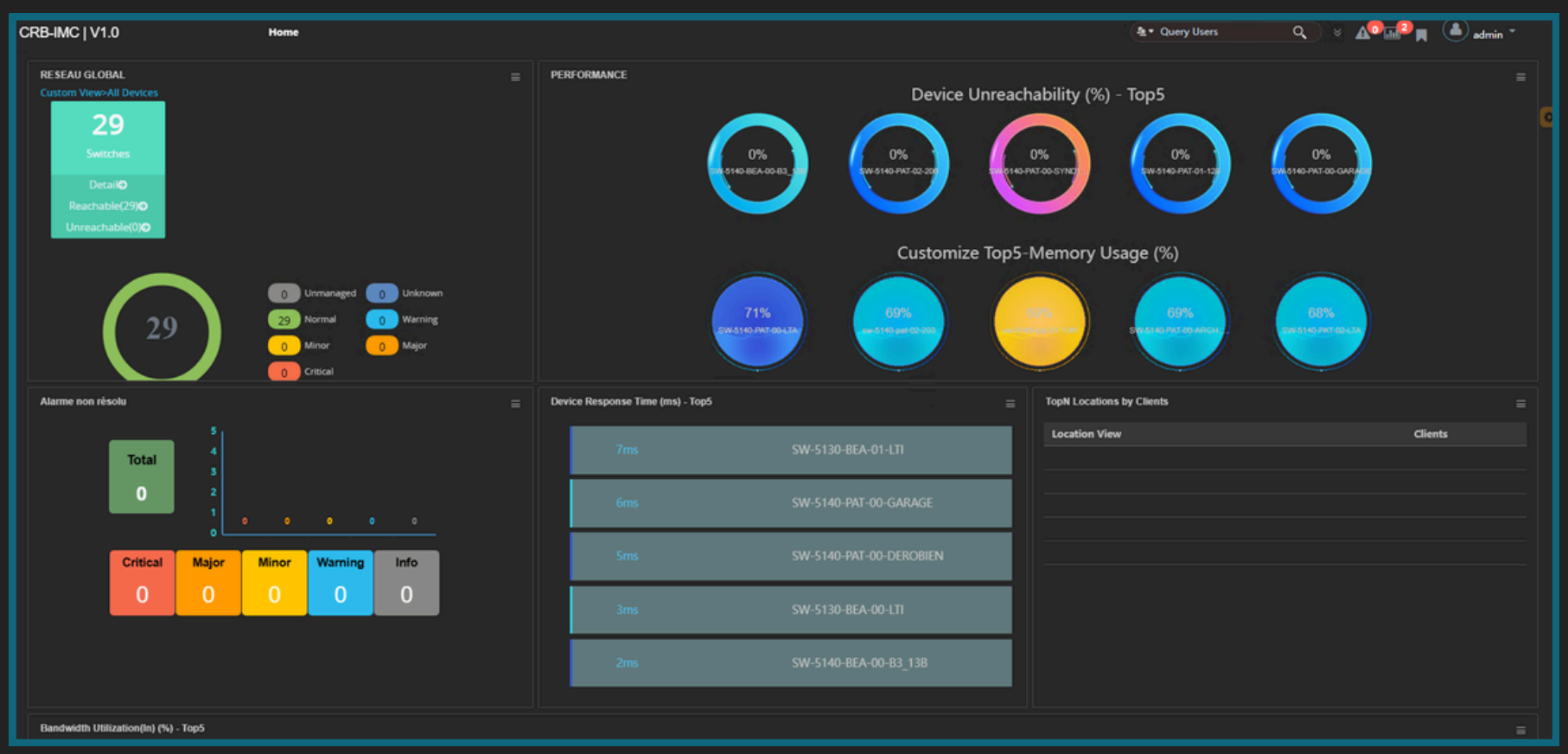
5.6 - Identification et corrections des bugs

Avant la mise en production de la solution HPE Intelligent Management Center, j'ai réalisé une phase de vérification afin d'identifier et corriger les principaux problèmes rencontrés lors des tests.

Le premier point concernait la mise à jour du firmware des switchs Hewlett Packard Enterprise. Certains équipements refusaient les mises à jour à cause d'une version trop ancienne du système interne (DOM). J'ai donc effectué une mise à niveau manuelle pour les rendre compatibles avec la plateforme.

Un second problème touchait l'interface de supervision : l'organisation des tableaux de bord ne se sauvegardait pas correctement. Après analyse et échange avec le support HPE, une correction a été appliquée au niveau de la base de données MySQL, ce qui a permis de résoudre le problème.

Enfin, j'ai constaté une consommation élevée de mémoire sur le serveur. J'ai donc désactivé certains modules inutiles afin d'optimiser les performances.
Cette phase m'a permis de comprendre l'importance des tests avant une mise en production, ainsi que la nécessité d'analyser et corriger les problèmes pour garantir un outil fiable et adapté aux besoins.



Activité 5.6 (bis)

Déploiement d'HPE IMC sur le parc Institutionnel

5.6 (bis) - *Scan sécurité complémentaire*

Une fois les premiers équipements ajoutés dans HPE IMC sur l'environnement de test, j'ai réalisé une étape essentielle de vérification en collaboration avec l'équipe sécurité de la Région Bretagne. L'objectif était de s'assurer qu'aucune mauvaise configuration ne présentait un risque pour l'infrastructure avant toute mise en production.

Le scan de sécurité a permis d'analyser les ports ouverts, les services actifs et les accès possibles vers le serveur de test. Lors de cette analyse, deux failles ont été identifiées : l'une concernait un protocole de chiffrement TLS vulnérable, et l'autre un problème lié au stockage des données sensibles. Ces deux points ont été corrigés immédiatement afin de garantir un environnement sécurisé.

Cette étape m'a permis de comprendre l'importance de vérifier systématiquement la sécurité d'un système, même dans un environnement de test, et de constater que la détection et la correction rapide de failles potentielles sont indispensables pour protéger l'infrastructure avant toute mise en production.

Région
BRETAGNE

SCAN SYSTEM DE SECURITE

04/02/2026

Table des matières

Activité 5.7

Déploiement d'HPE IMC sur le parc Institutionnel

5.7 - Présentation de l'environnement de test et validation du projet.

Une fois l'ensemble des tests réalisés et les principaux problèmes techniques corrigés, j'ai présenté l'environnement de test de la solution HPE Intelligent Management Center à la direction de la DNSI de la Région Bretagne. Cette présentation avait pour objectif de démontrer concrètement le fonctionnement de l'outil et de valider l'intérêt de son déploiement sur l'ensemble du réseau.

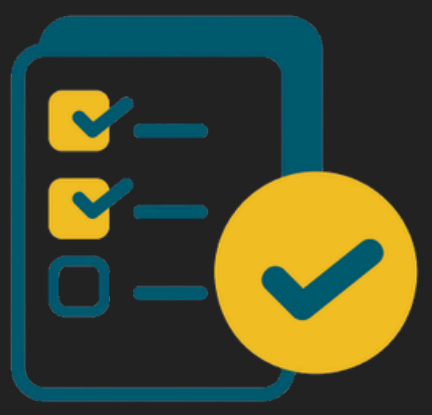
Lors de cette présentation, j'ai expliqué le rôle de la plateforme dans l'administration du nouveau parc de switchs Hewlett Packard Enterprise. J'ai notamment montré comment l'outil permet de centraliser la gestion des équipements, d'automatiser certaines tâches d'administration et de réaliser des actions sur plusieurs switchs en même temps. Les démonstrations portaient sur des opérations concrètes comme la création de VLAN, le déploiement d'ACL, la modification de paramètres sur les ports ou encore la gestion des configurations des équipements.

J'ai également présenté les résultats obtenus lors des tests réalisés sur l'environnement de validation, notamment en ce qui concerne la stabilité du logiciel, la consommation des ressources du serveur et les ajustements effectués pour optimiser son fonctionnement. Cette présentation permettait à la direction de disposer d'une vision claire de l'outil, de ses avantages et de son utilisation dans le contexte du réseau institutionnel.

L'objectif de cette étape était de confirmer que la solution répondait aux besoins de gestion du parc réseau et de valider officiellement le projet avant d'engager l'achat des licences nécessaires à la mise en production.

À l'issue de cette présentation, le projet a été validé par la direction, ce qui a permis d'envisager le déploiement de la solution à plus grande échelle.

La validation du projet ouvre ainsi la possibilité de déployer la plateforme sur l'ensemble du réseau institutionnel, mais également sur les infrastructures réseau des lycées gérés par la Région Bretagne. Cette étape marque donc la transition entre la phase de test et la mise en production de la solution.



Activité 5.8

Déploiement d'HPE IMC sur le parc Institutionnel

5.8 - Achat des licences et mise en relation avec le marché de la SPIE

Suite à la validation du projet par la direction de la DNSI de la Région Bretagne, l'étape suivante a consisté à procéder à l'acquisition des licences nécessaires pour la mise en production de la solution HPE Intelligent Management Center. Cette phase était essentielle pour pouvoir déployer officiellement l'outil sur l'ensemble des infrastructures concernées.
L'achat des licences s'est effectué dans le cadre du marché existant avec l'entreprise SPIE. Afin de respecter les procédures internes de la collectivité, la demande a été réalisée en passant par le Bau de Soie, qui est le point de gestion des demandes liées aux marchés publics et aux commandes informatiques.

Dans ce contexte, j'ai participé aux échanges avec le BPU afin de transmettre les informations nécessaires à la commande. Cela impliquait notamment de préciser le nombre de licences nécessaires en fonction du parc d'équipements à gérer. Le projet représentait un investissement important, estimé à environ 80 000 euros. La répartition des licences prévoyait environ 250 licences pour le réseau institutionnel et près de 1200 licences destinées aux infrastructures réseau des lycées gérés par la Région Bretagne.

Une fois la demande transmise et validée dans le cadre du marché existant, la commande a été traitée par le fournisseur. Les licences ont été reçues environ deux semaines après la demande, ce qui a permis de préparer la prochaine étape du projet, à savoir la mise en production de la solution sur les différents environnements.

Libellé	Référence	Prix net unitaire (BPU)	Qté	Prix net total
Réactivation Support sur licence en production				
Support 1 an - HPE IMC	U4AG4E	366,48 €	2	732,96 €
Extension licences				
Licence IMC - 50 Device *(extension de licence)*	JG749AAE	1 803,04 €	34	61 303,29 €
Support 1 an - HPE IMC	U4AG4E	366,48 €	34	12 460,35 €
Remise additionnelle sous conditions ci-dessous				- 16 913,65 €
		Total €HT		**56 850,00 €**
		Total €TTC		**68 219,99 €**

Libellé	Référence	Prix net unitaire (BPU)	Qté	Prix net total
Licence IMC - 50 Device *(extension de licence)*	JG749AAE	1 803,04 €	1	1 803,04 €
Support 1 an - HPE IMC	U4AG4E	366,48 €	1	366,48 €
Licence IMC - 50 Device *(extension de licence)*	JG749AAE	1 803,04 €	4	7 212,15 €
Support 1 an - HPE IMC	U4AG4E	366,48 €	4	1 465,92 €
Remise additionnelle sous conditions ci-dessous				- 947,59 €
		Total €HT		**9 900,00 €**
		Total €TTC		**11 880,01 €**

Activité 5.9

Déploiement d'HPE IMC sur le parc Institutionnel

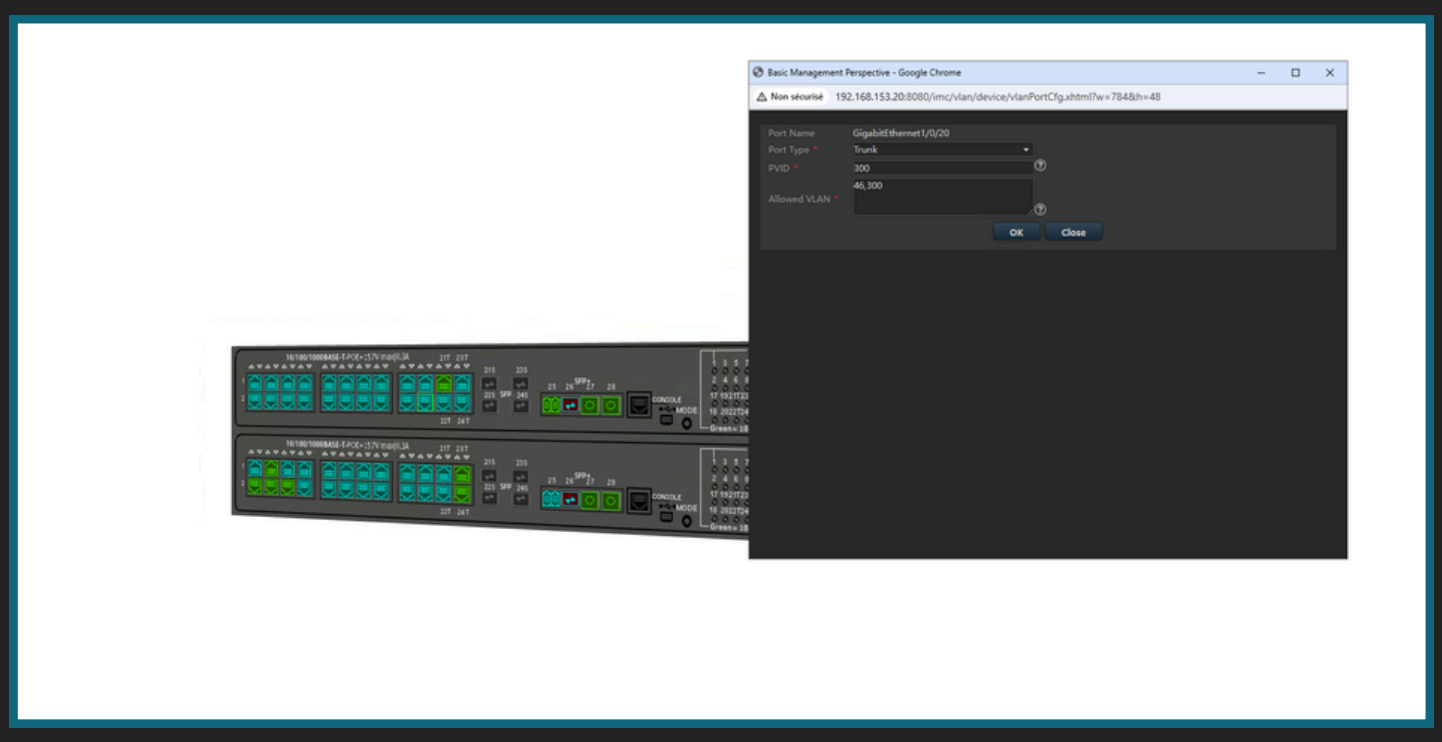
5.9 - Réception des licences et installation en production

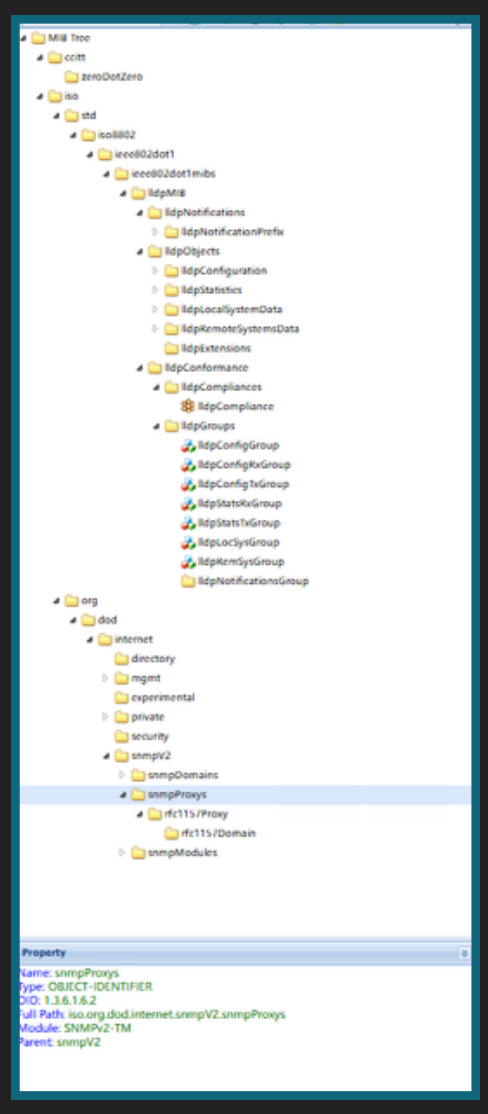
Après la réception des licences de HPE Intelligent Management Center, j'ai lancé la phase de déploiement en production pour le réseau de la Région Bretagne.

Avant l'installation, j'ai préparé un dossier technique pour demander la création des serveurs auprès de l'équipe système. Ce document précisait l'architecture, les ressources nécessaires et le rôle de chaque machine, en respectant les exigences internes.

L'architecture mise en place repose sur deux serveurs : un serveur sous Windows Server 2019 pour l'application, et un second sous Linux avec MariaDB pour la base de données. Cette séparation permet d'améliorer les performances, la maintenance et l'évolution de la solution.
Une fois les machines disponibles, j'ai installé la plateforme en m'appuyant sur les tests réalisés auparavant. J'ai appliqué les bonnes pratiques et corrigé les problèmes déjà identifiés afin d'assurer une installation stable.

Cette étape m'a permis de comprendre l'importance de la préparation et des procédures lors d'un déploiement en production, ainsi que la différence entre un environnement de test et une infrastructure réelle.

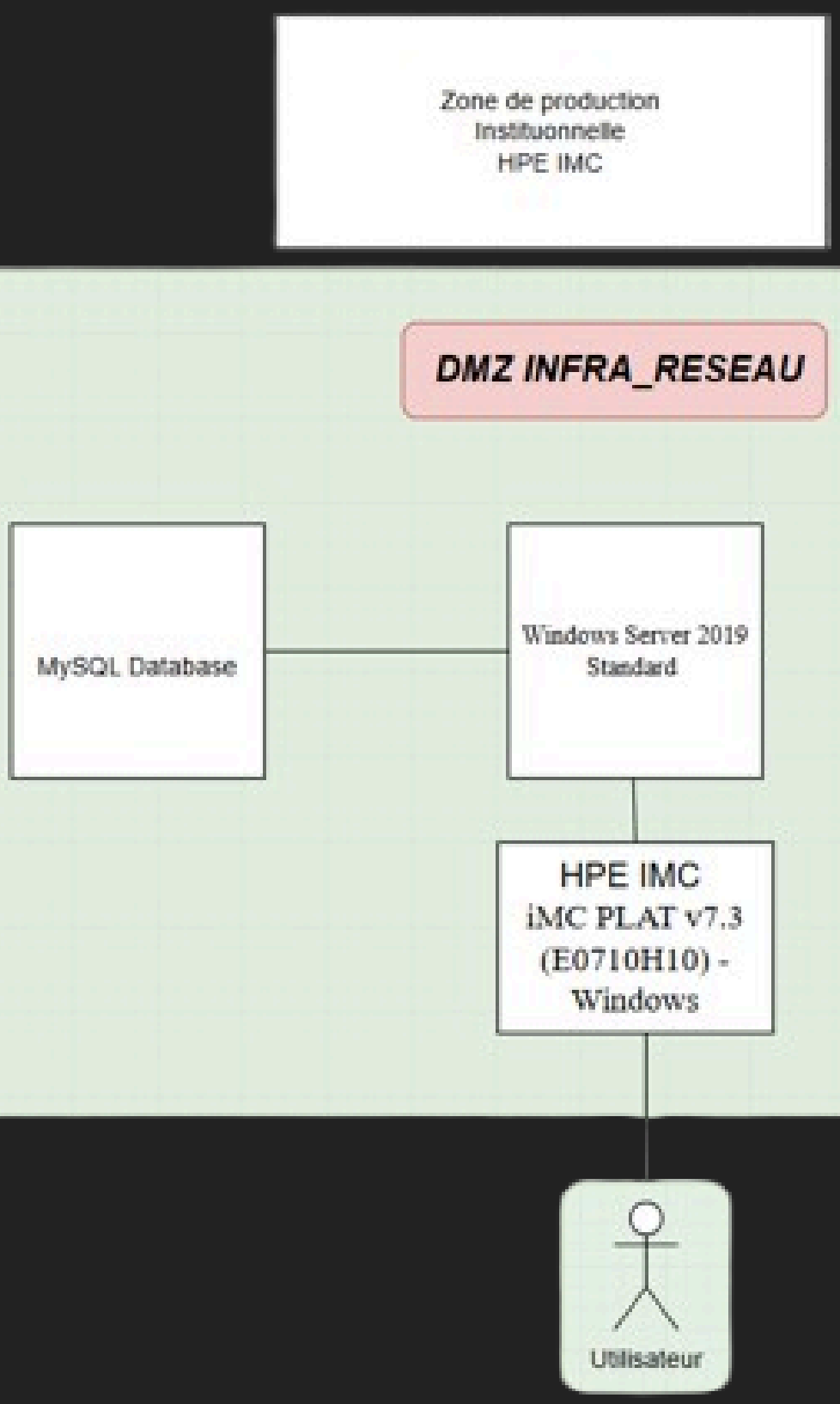




Activité 5.9 (bis)

Déploiement d'HPE IMC sur le parc Institutionnel

5.9 (bis) - Architecture de déploiement d'HPE IMC



Activité 5.10

Déploiement d'HPE IMC sur le parc Institutionnel

5.10 - Déploiement officiel du logiciel et présentation à l'équipe

Après l'installation complète de la solution HPE Intelligent Management Center sur les serveurs de production, j'ai réalisé le déploiement officiel sur le réseau de la Région Bretagne. Cette étape marquait l'entrée en exploitation de l'outil et sa mise à disposition pour l'administration centralisée du parc HPE, couvrant l'ensemble des équipements institutionnels et lycées.

Dans un premier temps, j'ai vérifié le bon fonctionnement de toutes les fonctionnalités essentielles : découverte des équipements, communication SNMPv3, profils d'écriture pour l'administration des switchs, ainsi que la supervision des interfaces et des VLAN. Toutes les corrections et ajustements identifiés lors des phases de test et de préproduction ont été appliqués afin de garantir la stabilité et la performance du logiciel. La base de données MariaDB a été validée pour assurer la continuité des tâches automatiques et la gestion des configurations centralisées.

Une fois le logiciel opérationnel, j'ai présenté la plateforme à l'équipe réseau et à l'équipe système. Cette présentation avait pour objectif de familiariser les collaborateurs avec les outils disponibles, d'expliquer les fonctionnalités principales et de montrer comment utiliser HPE IMC pour réaliser les opérations courantes. J'ai détaillé la gestion des VLAN, le déploiement des ACL, la modification des ports et la mise à jour des configurations sur plusieurs équipements simultanément. J'ai également expliqué l'organisation des dashboards et les bonnes pratiques à adopter pour éviter les erreurs ou la surcharge des serveurs.

Cette présentation a permis à l'équipe de mieux comprendre l'intérêt stratégique de la solution et la manière dont elle simplifie l'administration du parc réseau. Elle a également servi à renforcer la coordination entre les différents services et à formaliser les procédures d'utilisation pour les futures interventions.

Cette activité m'a appris à communiquer techniquement auprès d'une équipe, à expliquer clairement des concepts complexes et à mettre en valeur l'importance d'un outil centralisé pour la gestion efficace d'un réseau étendu. Elle m'a également confirmé l'importance de préparer soigneusement un déploiement pour assurer une transition fluide entre la phase de test et l'exploitation réelle.

Activité 5.11

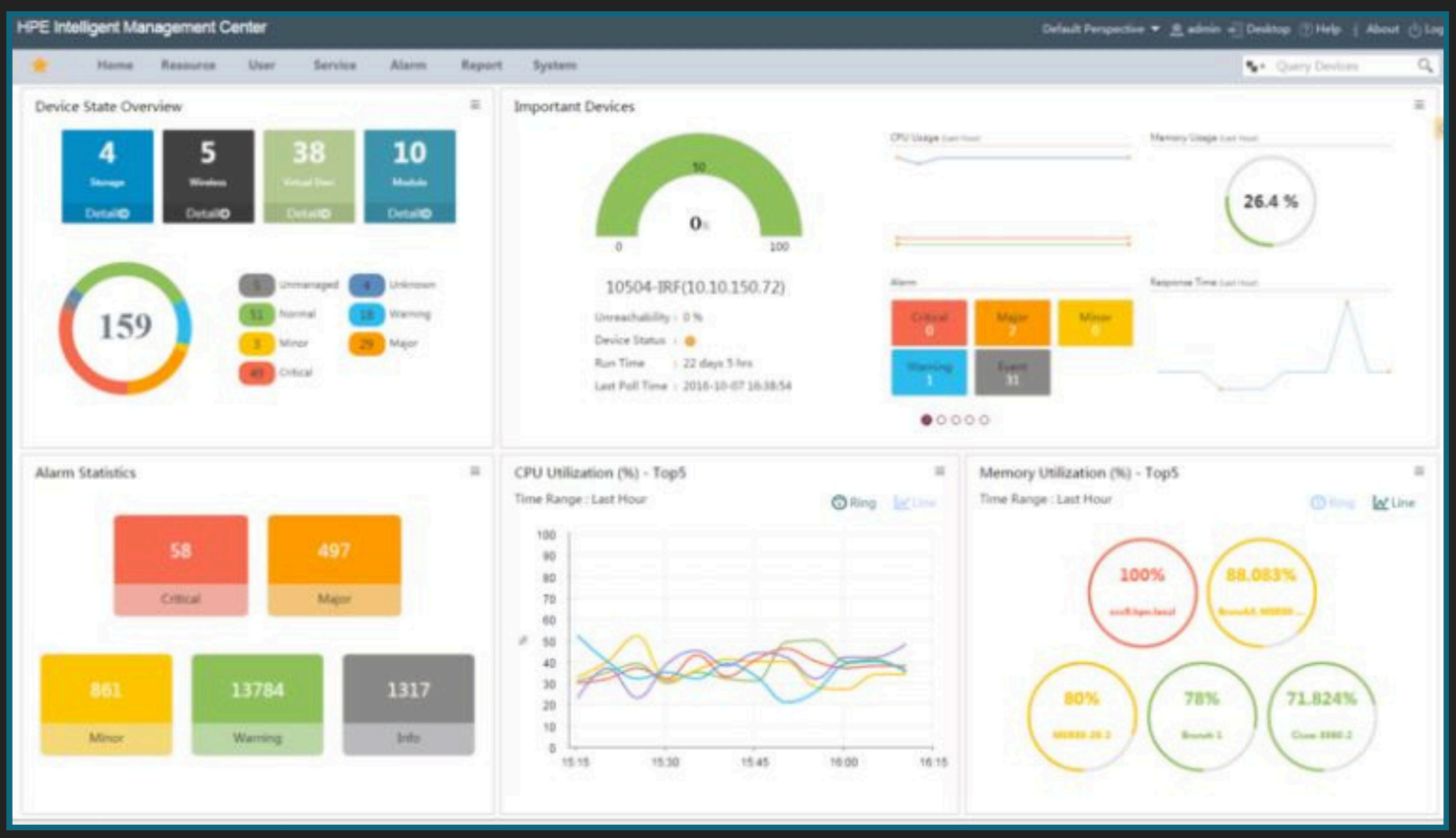
Déploiement d'HPE IMC sur le parc Institutionnel

5.11 - Conclusion de l'activité

Le déploiement officiel de HPE IMC a marqué l'aboutissement d'un projet technique complet, depuis l'étude initiale jusqu'à la mise en production sur le réseau de la Région Bretagne. Cette expérience m'a permis de suivre toutes les étapes d'un projet d'infrastructure à grande échelle : analyse des besoins, tests en environnement contrôlé, résolution de problèmes techniques, validation auprès de la direction, acquisition des licences et enfin installation et présentation à l'équipe.

J'ai pu constater concrètement l'importance d'une gestion centralisée des équipements réseau, non seulement pour simplifier les tâches d'administration, mais aussi pour assurer la sécurité, la cohérence et la performance de l'infrastructure. Travailler sur ce projet m'a permis de développer mon autonomie, ma rigueur et ma capacité à anticiper les contraintes techniques et organisationnelles.

Cette activité m'a également appris à combiner des compétences techniques avec des démarches administratives et de coordination, en tenant compte à la fois des besoins des utilisateurs, des équipes techniques et des exigences d'une collectivité territoriale. Elle a renforcé ma compréhension des outils de supervision et d'administration, tout en me donnant une vision globale de la gestion d'un réseau institutionnel moderne.



Activité 6

Installation d’une salle de visio-conférence avec VIDÉLIO

6.1 - Introduction du projet
6.2 - Notre rôle dans le cadre de l’intervention
6.3 - Installation des équipements
6.4 - Installation des équipements et configuration
6.5 - Réalisation des test
6.6 - Conclusion de l’activité

Activité 6.1

Installation d'une salle de visio-conférence avec VIDÉLIO

6.1 - Introduction du projet

Dans le cadre de l'amélioration des outils de communication, la Région Bretagne a souhaité déployer une salle de visioconférence sur le site de Patton. L'objectif était de tester une solution complète dans une première salle, afin de pouvoir ensuite la reproduire et l'étendre à d'autres espaces si les résultats étaient concluants.

Pour ce projet, la Région a fait appel à la société Videlio, spécialisée dans l'intégration de solutions audiovisuelles et de visioconférence professionnelles. Leur intervention consistait à installer un système complet comprenant des microphones, des équipements audio, un grand écran, ainsi que des caméras capables de couvrir l'ensemble de la salle avec des mouvements fluides et automatisés.

L'équipe réseau joue un rôle essentiel dans ce type de projet. En amont, nous avons dû préparer l'infrastructure en ouvrant les flux nécessaires selon le cahier des charges fourni, et en définissant les VLAN à utiliser pour isoler correctement les équipements de visioconférence. Pendant l'intervention, nous avons également accompagné les équipes de Videlio pour leur expliquer la configuration réseau en place, notamment sur les switchs, afin d'assurer une intégration propre et fonctionnelle.

L'installation s'est déroulée sur trois jours, durant lesquels les équipes de Videlio ont été accompagnées par notre équipe. Ce travail en collaboration a permis de mettre en place une solution complète, propre et opérationnelle, répondant aux besoins de communication de la Région.

videlio
Experiences that move you

Activité 6.2

Installation d'une salle de visio-conférence avec VIDÉLIO

6.2 - Configuration des commutateurs

Dans le cadre de l'installation de la salle de visioconférence, j'ai configuré et déployé deux switchs HPE 5140 en stack en utilisant la technologie IRF (Intelligent Resilient Fabric). L'IRF permet de regrouper plusieurs switchs physiques en un seul switch logique. Concrètement, les deux switchs fonctionnent comme une seule entité réseau : ils partagent la même configuration, le même plan de contrôle et une seule adresse IP pour la gestion, ce qui simplifie l'administration et augmente la résilience.

Grâce à l'IRF, le trafic entre les deux switchs est optimisé et équilibré automatiquement, et si l'un des switchs venait à tomber en panne, le second continue de fonctionner, assurant ainsi la continuité du réseau. Cette architecture a été particulièrement utile pour la salle de visioconférence, où la disponibilité et la qualité du réseau sont essentielles pour les flux audio et vidéo.

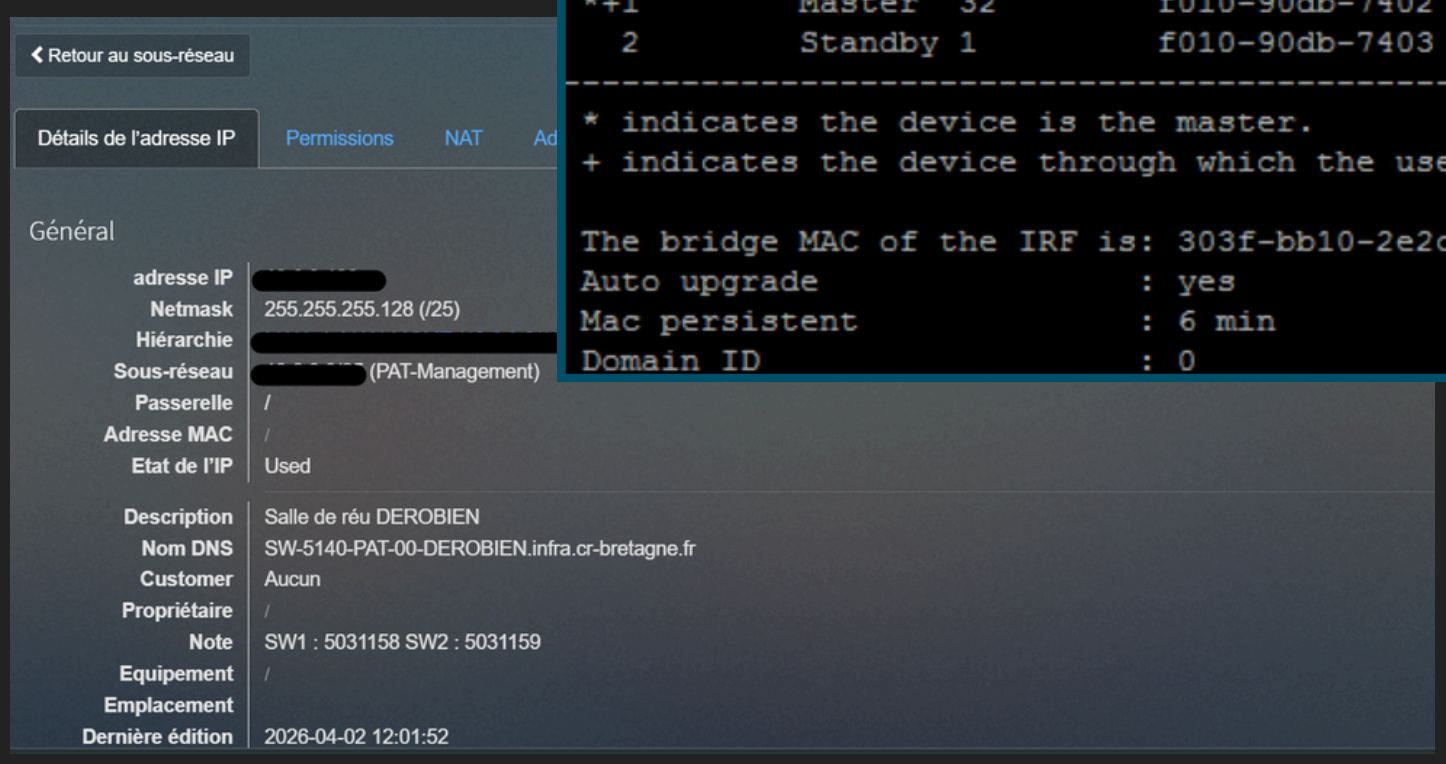
Avant l'installation sur site, j'ai configuré le VLAN dédié MEETING_SÉCURISÉ (VLAN 576) pour isoler le trafic des équipements de visio, activé le PoE sur les ports destinés aux caméras et autres périphériques, nommé les switchs selon la charte de l'équipe SINFRA et enregistré leur adresse IP dans notre serveur RADIUS pour l'authentification sécurisée. Une série de tests a été effectuée pour vérifier la connectivité, le bon fonctionnement du VLAN et du PoE, ainsi que la synchronisation entre les switchs en stack IRF.

Cette configuration m'a permis de mettre en place un réseau robuste et sécurisé pour la salle, tout en découvrant concrètement le fonctionnement et les avantages de l'IRF pour la gestion des infrastructures réseau.

Vérification du bon fonctionnement du lien IRF entre les deux équipements

```
<SW-5140-PAT-00-DEROBIEN>show irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        f010-90db-7402  7333887
  2         Standby 1         f010-90db-7403  7333888
-------------------------------------------------
* indicates the device is the master.
+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 303f-bb10-2e2c
Auto upgrade                : yes
Mac persistent              : 6 min
Domain ID                   : 0
```



Réservation de l'adresse IP du commutateur en DHCP

Activité 6.3

Installation d’une salle de visio-conférence avec VIDÉLIO

6.3 - Notre rôle dans le cadre de l’intervention

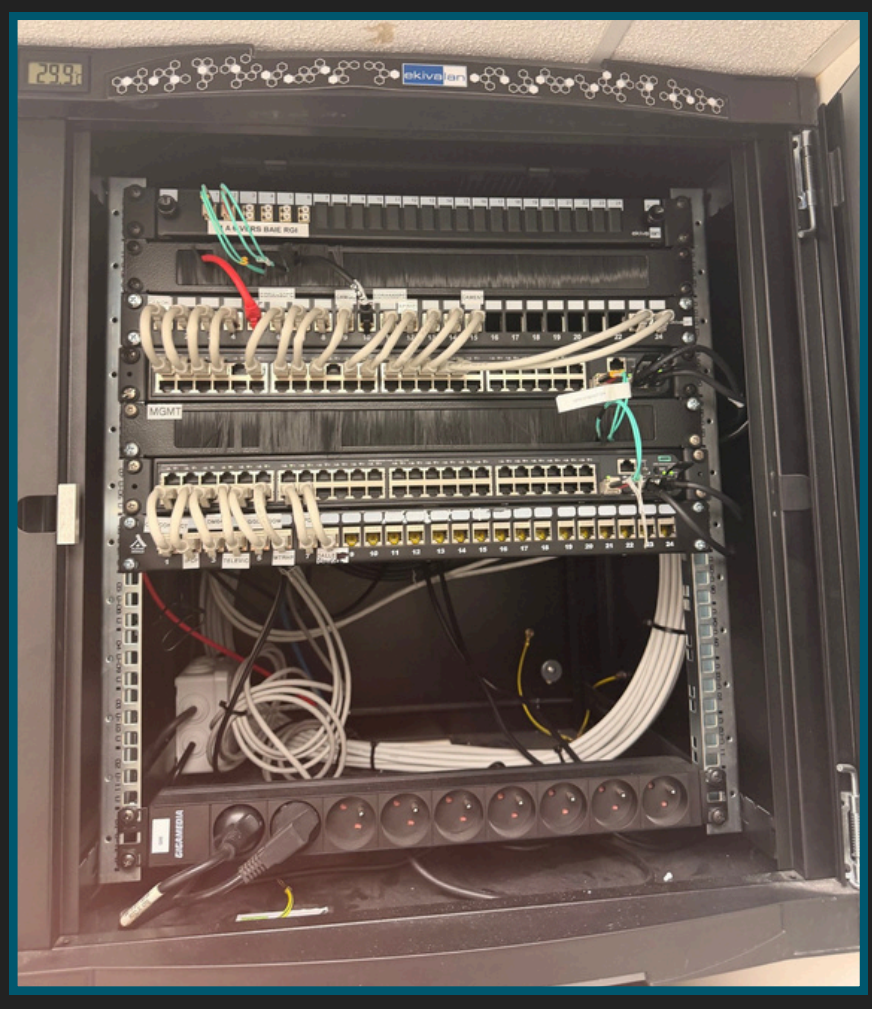
Dans le cadre de ce projet, mon rôle, au sein de l’équipe réseau, a été de préparer et d’accompagner l’intégration des équipements de visioconférence sur l’infrastructure existante.

Nous avons d’abord réalisé l’ouverture des flux réseau nécessaires au bon fonctionnement de la solution, en respectant le cahier des charges fourni par Videlio. Cette étape est essentielle pour permettre la communication entre les équipements (caméras, microphones, systèmes de visioconférence) et les services externes.

J’ai également contribué à l’installation de la baie réseau dédiée, avec la mise en place de switchs HPE 5140 48G, configurés par mes soins. Les équipements ont été installés en stack de deux switchs, ce qui permet d’assurer une meilleure redondance et une gestion simplifiée.
En parallèle, j’ai participé à la configuration des VLAN nécessaires pour isoler les flux liés à la visioconférence, afin de garantir à la fois la sécurité et la qualité de service.

Enfin, nous avons assuré un rôle de supervision pendant toute la durée des travaux. Cela consistait à suivre l’avancement de l’installation, vérifier la bonne intégration des équipements sur le réseau et accompagner les équipes sur place en cas de besoin.

Cette intervention m’a permis de mieux comprendre l’importance du rôle de l’équipe réseau dans un projet global, où plusieurs intervenants travaillent ensemble pour mettre en place une solution complète.



Activité 6.4

Installation d’une salle de visio-conférence avec VIDÉLIO

6.4 - Installation des équipements et configuration

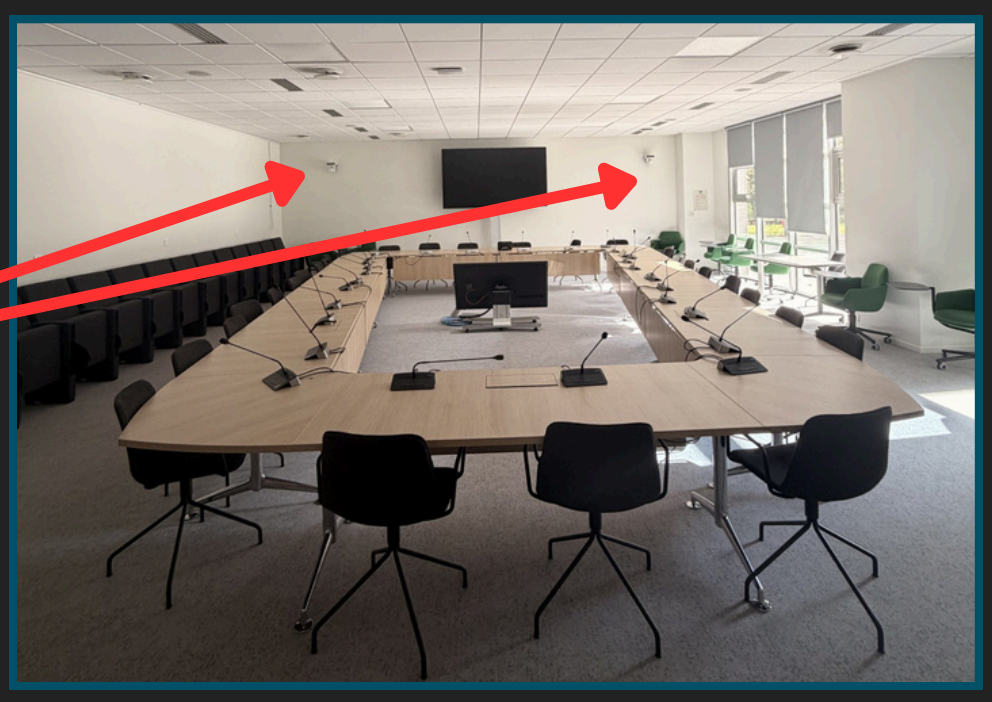
Une fois les switchs HPE 5140 installés et configurés, il était temps pour l’équipe VIDÉLIO de procéder au calibrage et à la configuration de leurs équipements : caméras, micros, écrans et consoles de contrôle. Nous avons pu assister à cette étape pour vérifier que tout correspondait à ce qui était attendu lorsque le projet avait été programmé.

Les trois caméras installées sont entièrement rotatives et offrent une haute résolution. Elles sont capables de centrer automatiquement l’image sur l’intervenant qui parle, grâce à la détection du son de son micro. Chaque caméra est directement reliée au switch PoE situé dans la baie informatique, installée dans une pièce isolée de la salle de réunion, ce qui leur permet d’être alimentées et connectées sans câbles supplémentaires.

Pendant cette phase, j’en ai profité pour étiqueter chaque câble RJ afin de faciliter toute intervention future dans la baie et de pouvoir identifier rapidement chaque connexion en cas de besoin. Parallèlement, nous avons vérifié que tous les flux réseau fonctionnaient correctement, notamment ceux provenant du concentrateur audio et des différents périphériques. Chaque connexion a été testée afin de confirmer que les VLAN, les adresses IP et le PoE mis en place précédemment fonctionnaient correctement avec les équipements VIDÉLIO.

La documentation du prestataire a été scrupuleusement respectée, et l’ensemble des flux passait sans problème. À ce stade, il ne restait plus qu’à effectuer les tests finaux pour valider pleinement le fonctionnement de la salle.

Cette étape a été importante pour garantir que l’infrastructure réseau préparée par l’équipe réseau et les équipements VIDÉLIO étaient parfaitement compatibles et opérationnels, tout en assurant une organisation claire et un accès simplifié pour toute intervention future.



Activité 6.5

Installation d’une salle de visio-conférence avec VIDÉLIO

6.5 - Réalisation des test

Une fois l’ensemble des équipements installés et configurés, nous avons procédé aux tests fonctionnels de la salle de visioconférence. Chaque participant a pris place et parlé afin de vérifier que les caméras centraient correctement l’image sur l’intervenant qui s’exprime. Nous avons également testé un appel via Teams pour contrôler la fluidité et la synchronisation du flux, même pour les participants connectés à distance.

Lors de ces tests, des ajustements ont été réalisés sur la dalle sonore ainsi que sur les capteurs des micros afin d’améliorer la détection de la voix et la qualité audio globale. Finalement, la dalle sonore n’était pas nécessaire pour une salle de cette taille et a été retirée. Les caméras ont été paramétrées pour pointer uniquement en fonction de la localisation du micro qui prend la parole, garantissant ainsi un suivi précis et naturel des intervenants.

Ces tests ont permis de valider la configuration finale de la salle, d’assurer une expérience de visioconférence fluide et fonctionnelle, et de confirmer que les ajustements techniques répondaient aux besoins du projet.

Activité 6.6

Installation d’une salle de visio-conférence avec VIDÉLIO

6.6 - Conclusion de l’activité

L’installation de la salle de visioconférence avec VIDÉLIO m’a permis de participer à toutes les étapes du projet, depuis la configuration des switchs HPE 5140 et la mise en place des VLAN et du PoE, jusqu’à l’installation des équipements par le prestataire. J’ai pu assister au calibrage et à la configuration des caméras, micros et autres dispositifs réalisés par VIDÉLIO, ce qui m’a permis de comprendre le fonctionnement d’un système de visioconférence professionnel et d’observer les bonnes pratiques mises en œuvre.

Cette activité m’a également donné l’occasion de travailler en collaboration avec une équipe externe tout en appliquant les bonnes pratiques de l’infrastructure réseau interne, de gérer la connectivité et l’alimentation des équipements, et d’assurer un suivi clair grâce à l’étiquetage des câbles et à l’organisation de la baie.

En conclusion, ce projet illustre l’importance de la coordination technique, de la rigueur dans la préparation et la configuration du réseau, ainsi que de l’observation attentive des systèmes pour comprendre leur fonctionnement, garantissant ainsi une installation fonctionnelle et professionnelle.

videlio
Experiences that move you

Veille technologique

L’IA appliquée à la cybersécurité

“L’exemple de Fortinet”

VEILLE TECHNOLOGIQUE

L’IA appliquée à la cybersécurité “L’exemple de Fortinet”

FortiAI est une solution développée par Fortinet qui utilise l’intelligence artificielle pour renforcer la cybersécurité des réseaux et des systèmes. Elle est conçue pour détecter automatiquement les menaces, protéger les données sensibles et les environnements utilisant l’IA, et accélérer les réponses aux incidents.

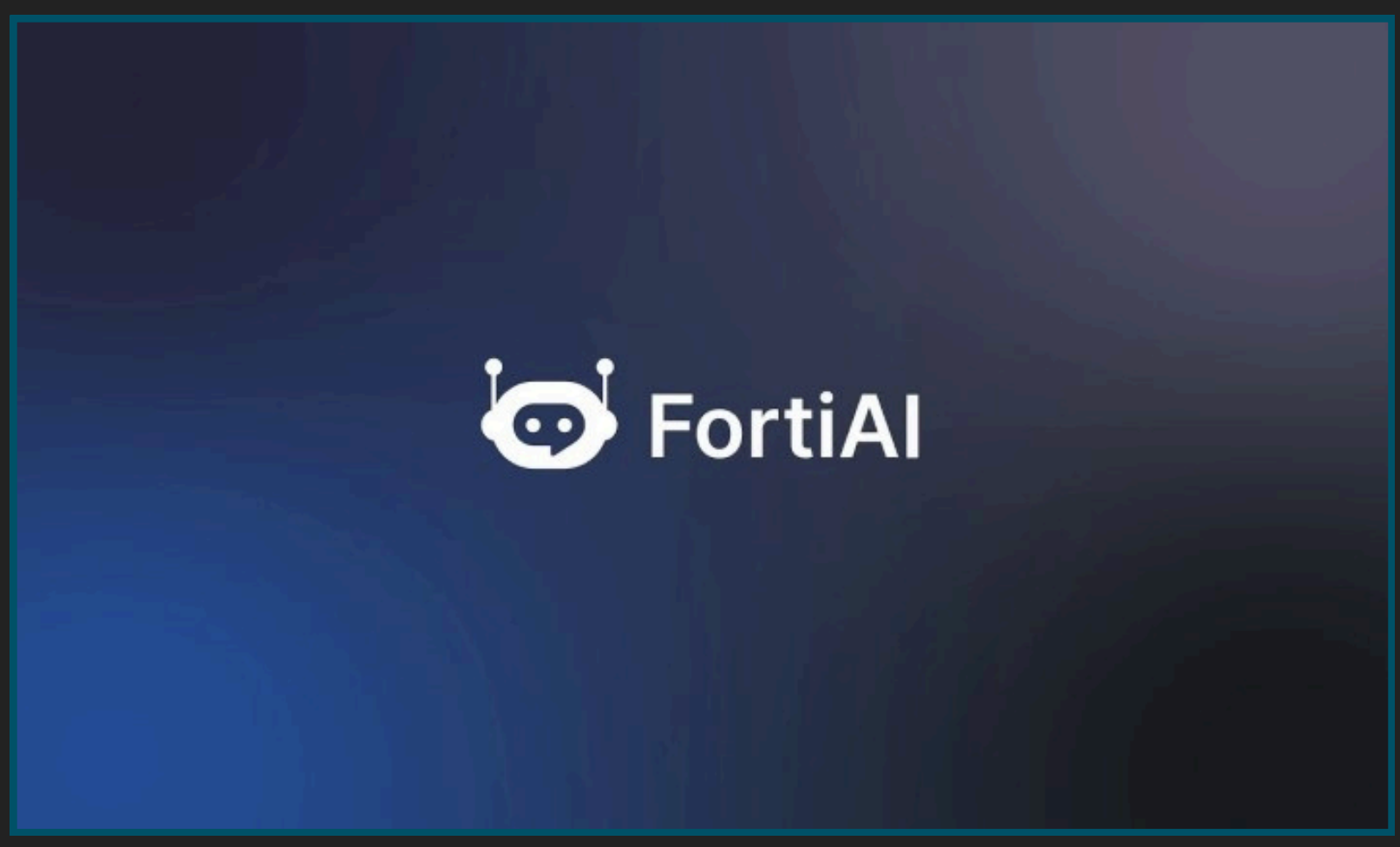
Contexte à la Région Bretagne:

La Région Bretagne utilise déjà des pare-feu Fortinet pour sécuriser ses réseaux. Ces firewalls gèrent le trafic, appliquent des règles de sécurité et protègent l’infrastructure contre les attaques externes. Pour le moment, la Région n’a pas adopté l’usage de FortiAI, mais je me renseigne activement sur cette solution afin de comprendre son fonctionnement et son intérêt potentiel pourle monde de la cybersécurité.

Fonctionnement et risques:

FortiAI analyse les flux réseau et les comportements des systèmes en temps réel pour détecter des anomalies et menaces. L’IA peut automatiser certaines réponses pour réduire le temps d’intervention. Cependant, son déploiement sur un réseau de production comporte des risques potentiels :

- Mauvaise configuration ou règle mal appliquée pouvant bloquer des flux essentiels ou créer des interruptions de service.
- Impact sur la continuité du réseau si une réponse automatique isole par erreur des systèmes critiques.



VEILLE TECHNOLOGIQUE

L’IA appliquée à la cybersécurité “L’exemple de Fortinet”

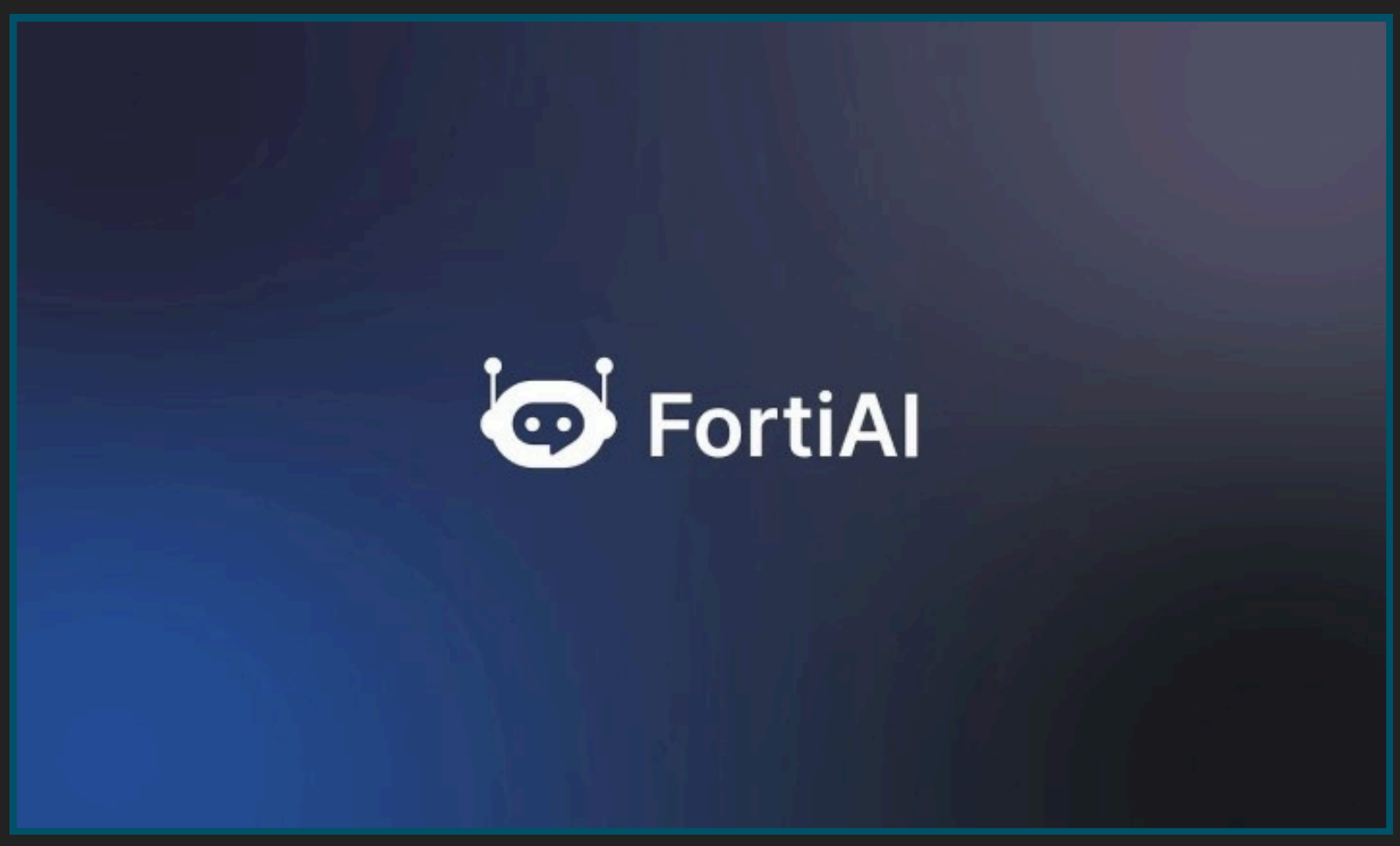
Depuis environ un an, je m’intéresse à **FortiAI** et à son potentiel dans le domaine de la cybersécurité. Ce sujet me passionne car il montre comment l’intelligence artificielle peut renforcer la sécurité des réseaux tout en automatisant certaines tâches, qui est un enjeu crucial pour des infrastructures complexes.

Sur un grand réseau, l’intérêt de FortiAI est particulièrement marqué :

Détection rapide et continue des menaces : sur un réseau étendu avec de nombreux firewalls et serveurs, il serait difficile pour une équipe humaine de suivre tous les flux. FortiAI peut analyser en temps réel les comportements suspects et alerter ou réagir immédiatement.

Réduction de la charge opérationnelle : l’IA permet d’automatiser certaines réponses et d’identifier les anomalies avant qu’elles n’affectent la production, réduisant ainsi le risque d’erreur humaine.

En anticipant les menaces et en signalant les mauvaises configurations, FortiAI peut aider à maintenir la continuité des services critiques.
Même si la Région Bretagne n’a pas encore adopté cette solution, cette veille m’a permis de comprendre ses applications concrètes, d’évaluer ses avantages et limites, et d’apprécier l’importance d’outils innovants pour sécuriser efficacement de grands réseaux professionnels.



CONCLUSION GENERALE

Ces deux années d'alternance à la Région Bretagne, au sein du service SINFRA de la DNSI, ont été très formatrices et m'ont permis de grandir sur le plan professionnel et personnel. Travailler dans un organisme public m'a appris à m'adapter à des procédures strictes, à respecter des règles précises et à comprendre l'importance de la rigueur dans chaque tâche.

Au fil des projets, j'ai renforcé mon organisation personnelle : planifier lesinterventions, suivre l'avancement des déploiements, préparer et tester les équipements avant chaque mise en service. Cette expérience m'a appris à gérer mon temps efficacement, à anticiper les problèmes et à prioriser les actions pour que tout fonctionne correctement, même dans un environnement complexe.

Travailler dans un organisme public m'a également permis de développer mon sens des responsabilités et de comprendre l'importance de chaque action sur le fonctionnement global du service. J'ai appris à collaborer avec différentes équipes, à communiquer clairement et à coordonner mes interventions avec des prestataires externes et des collègues, pour garantir la réussite des projets.

Enfin, cette alternance m'a donné confiance en mes capacités à évoluer dans un environnement technique exigeant, tout en renforçant mon autonomie, ma rigueur et ma capacité à m'organiser. Ces deux années constituent un socle solide pour ma future carrière dans le domaine des réseaux et de l'infrastructure informatique, et elles m'ont permis de mieux comprendre les exigences et le fonctionnement d'un service informatique public.

Région
BRETAGNE